Author: Klitou, Demetrius
Title: Privacy-invading technologies : safeguarding privacy, liberty & security in the 21st century
Date: 2012-12-14

Privacy-Invading Technologies: Safeguarding Privacy, Liberty & Security in the 21st Century

PROEFSCHRIFT

er verkrijging van
de graad van Doctor aan de Universiteit Leiden,
op gezag van Rector Magnificus prof. mr. P.F. van der Heijden, vol-
gens besluit van het College voor Promoties
te verdedigen op vrijdag 14 december 2012
klokke 11.15 uur

door

Demetrius Klitou

geboren te Philadelphia, U.S.A in 1981

Promotiecommissie:

Promotoren:	Prof. dr. A.H. J. Schmidt
	Prof. dr. G.J. Zwenne
Overige leden:	Prof. dr. J.A. Cannataci (Rijksuniversiteit Groningen)
	Prof. dr. M. Hildebrandt (Radboud Universiteit Nijmegen)
	Prof. dr. D. Hirsch (Capitol University Law School, Columbus OH, U.S.A)
	Prof. dr. S. van der Hof
	Dr. J.J.F.M. Borking
	Dr. B.W. Schermer

This dissertation is dedicated to my mother for her long-term support, and to Angie for her unwavering patience and encouragement.

Preface

I find the implications of tomorrow's information society and the advancement of the latest technologies capable of infringing upon the right to privacy and individual liberty extremely relevant. As a result, I decided to write a PhD dissertation on the subject.

The discourse in privacy and technology is a legal and political issue, and is more and more a matter of international relations and human rights law. The interplay between politics, ethics, social issues and technology/technological development is a growing phenomenon. Recent examples of the intersection of (international) politics, law, technology and privacy involve the Passenger Name Record (PNR) dispute between the US and EU, the potential widespread deployment of body scanners and the clash between the European Parliament and EU Council of Ministers over the US-EU SWIFT agreement.[1]

Privacy is a fundamental human right, and deserves just as much attention as any other human right. While there are certainly more grave human rights violations across the globe, particularly in Asia and Africa, here in the West, predominantly in the US and the UK, the threat upon the right to privacy and liberty thereof at the hands of those who control advanced technology is and will remain the story of the early 21st Century. This is true, I argue, even in the midst of other highly significant and pressing matters, such as the global fight against terrorism, nuclear proliferation, climate change, environmental disasters and the ongoing global economic crisis. Indeed, as technology increasingly advances, in terms of its capabilities in intruding upon privacy, collecting and analyzing personal data and conducting mass surveillance, I believe the right to privacy will equally become more and more significant.

It is perhaps during crises, particularly as a result of a major terrorist attack, that governments (and citizens) are more likely inclined to support the further development and deployment of technologies capable of safeguarding security. And, in a post-9/11 world, this has indeed occurred. However, the same technologies are often also capable of seriously intruding upon privacy and other civil liberties.

It is important to note that I am certainly not against technology, nor against governments using technology. This PhD dissertation does not serve to scaremonger. On the

---

1 The Society for Worldwide Interbank Financial Telecommunication (SWIFT) manages a global network for exchanging financial messages necessary for facilitating the execution of payment orders/transactions between financial institutions. The US-EU SWIFT agreement allows for the transfer of SWIFT transaction information from the EU to the US.

contrary, it serves to point out both the wanted benefits and unwanted privacy threats of the latest technologies and recommend how to prevent those threats. I am a technology enthusiast and a supporter of the vast number of digital services available, from Twitter to Google. I also especially recognize the infinite possibilities and benefits of technology for society and its well-being. Indeed, for example, the advancement of ICT can address major global societal challenges and provide benefits in terms of commerce, health, democratic participation, social inclusion, environment, and convenience. I am aware that technologies can help governments to serve citizens. Governments use ICT to enhance public security and personal safety and to save lives, for instance, by providing communication capabilities and vital information to first responders, such as digital maps, driving directions, medical information and images. Governments can also use identification technologies, advanced imaging technologies and technologies capable of mass surveillance for better ensuring public/national security.

However, as technology rapidly advances and becomes evermore pervasive in society, the way and degree to which privacy and liberty may be violated also advances. The right to privacy is becoming evermore difficult to enforce. This has led some to argue that privacy (at least as we know it) will end in the near future, if we do nothing about it (Garfinkel, 2001), or is already on its way to ending (Whitaker, 2000; Holtzman, 2006; O'Hara and Shadbolt, 2008), or even has already ended so get over it,[2] and besides what's the use of doing anything about it. At the Centre for Law in the Information Society (eLaw@Leiden), Bart Schermer more specifically argues that privacy will cease to exist in 20 years (2007, 2010). All the same, there is also the strong disbelief that privacy can be concretely ensured in the near future. For some, therefore, the end of privacy and the right thereof is simply inevitable.

For these reasons, now more than ever, I believe it is time to thoroughly tackle the great challenges and threats posed by the latest technologies on the right to privacy and other civil liberties, and to thwart the prediction that privacy will end soon. I for one also believe that the immense benefits of technology do not have to come at the undesirable expense of privacy and other liberties.

Demetrius Klitou
January, 2012

2 For example, Scott McNealy, the former CEO of Sun Microsystems, famously once declared, over a decade ago, "You have zero privacy anyhow, get over it". see Sprenger, Polly. "Sun on Privacy: 'Get over it'" (Wired, 26 January, 1999), available at: http://www.wired.com/politics/law/news/1999/01/17538

Privacy-Invading Technologies: Safeguarding Privacy, Liberty & Security in the 21st Century

Table of Contents

List of Abbreviations

ABC	Acceptable Behaviour Contract
ACLU	American Civil Liberties Union
ACPO	Association of Chief Police Officers
ALPR	Automatic License Plate Recognition
AI	Artificial Intelligence
AMA	American Medical Association
AMDA	American Medical Directors Association
ASB	Anti-social Behaviour
ASBO	Anti-social Behaviour Orders
ATD	Automatic Threat Detection
ATM	Automatic Teller Machine
BAT	Best Available Technique
CALEA	Communications Assistance for Law Enforcement Act 1994
CAPPS	Computer Assisted Passenger Prescreening System
CCTV	Closed-Circuit Television
CIA	Central Intelligence Agency
CNN	Cable News Network
COPPA	Children's Online Privacy Protection Act
CPNI	Customer Proprietary Network Information
CTIA	Cellular Telecommunications and Internet Association
CTTL	Clandestine Tagging, Tracking, and Locating
DARPA	Defense Advanced Research Projects Agency
DHS	Department of Homeland Security
DNA	Deoxyribonucleic Acid
DNS	Domain Name System
DPA	Data Protection Act 1998
EC	European Commission
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
ECPA	Electronic Communications Privacy Act

EDPS	European Data Protection Supervisor
EHR	Electronic Health Records
EPC	Electronic Product Code
EPIC	Electronic Privacy Information Center
ETD	Explosive Trace Detection
EU	European Union
FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FDA	Food & Drug Administration
FEC	Federal Election Commission
FIP	Fair Information Principle
FIPPS	Fair Information Practice Principles
FISA	Foreign Intelligence Surveillance Act
FTC	Federal Trade Commission
GAO	Government Accountability Office
GIS	Geographic Information Systems
GLN	Global Location Number
GPRS	General Packet Radio Service
GPS	Global Positioning System
GWOT	Global War on Terror
HIM	Human-Implantable Microchip
HIPAA	Health Insurance Portability and Accountability Act
HRA	Human Rights Act 1998
HSS	HyperSonic Sound
ICCPR	International Covenant of Civil and Political Rights
ICO	Information Commissioner's Office
ICT	Information and Communication Technology
ID	Identification
IED	Improvised Explosive Devices
IID	Improvised Incendiary Device
IoT	Internet of Things
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ITS	Intelligent Transport Systems
ISE	Information Sharing Environment
ISO	International Organization for Standardization
IT	Information Technology

KHz	Kilohertz
LBA	Location-Based Advertising
LBS	Location-Based Service
LEXID®	Lobster-Eye X-ray Imaging Device
LF	Low Frequency
LML	Legal Machine Language
LNL	Legal Natural Language
LRAD	Long-Range Acoustic Devices
LPR	Legal Permanent Resident
LVA	Layered Voice Analysis
MCD	Mobile Computing Device
NGO	Non-governmental Organization
NGR	Next Generation Robot
NIR	National Identity Register
NIST	National Institute of Standards and Technology
NORAD	North American Aerospace Defense Command
PBD	Privacy by Design
OECD	Organization for Economic Co-operation and Development
PC	Personal Computer
PDA	Personal Digital Assistant
PET	Privacy-Enhancing Technology
PIA	Privacy Impact Assessment
PIN	Personal Identification Number
PIT	Privacy-Invading Technology
PLD	Personal Locating Device
PNR	Passenger Name Record
PSCO	Police Support Community Officers
PUF	Physical Unclonable Function
P3P	Privacy Preferences Project
R&D	Research and Development
RFID	Radio Frequency Identification
RIPA	Regulation of Investigatory Powers Act 2000
RTD	Research and Technological Development
SERS	Surface Enhanced Raman Spectroscopy
SOP	Standard Operating Procedure
TATP	Triacetone Triperoxide
TNT	Trinitrotoluen
TRE	Tag Read Events
TSA	Transportation Security Administration

TSO	Transportation Security Officer
UAV	Unmanned Aerial Vehicle
UK	United Kingdom
UDHR	United Nations Declaration of Human Rights
UDI	User-Driven Innovation
UHF	Ultra High Frequency
UHID	Universal Healthcare Identifier
UN	United Nations
US	United States
VIRAT	Video Image Retrieval and Analysis Tool
VCR	Video Cassette Recorder
VSD	Value-Sensitive Design
VSS	Voting System Standards
WBI	Whole Body Imaging
WTMD	Walk-Through Metal Detector

PART I

1. Introduction
2. Privacy, liberty & security
3. Criteria for assessing the adequancy of a legal frame work in terms of protecting privacy

1 Introduction

1.1 PROBLEM STATEMENT

Since the beginning of the 21st Century, as a result of the growing development and deployment of technology, the following new privacy issues or threats have arisen in the US and the UK/EU:

- A digital data trail is generated by each and every person and automatically stored.
- Law enforcement agencies are routinely using mobile phones as a tool to either track people or record their geographic location in real-time. Mobile phones are also capable of being used to record conversations (even when turned off).[3]
- Vehicles are being tracked via ALPR systems and/or via GPS tracking devices without a warrant.
- Banks have begun testing the use of fingerprint scanners to authenticate identity, while supermarkets are also testing biometric payment systems.
- RFID microchips are being embedded within a variety of consumer goods, and RFID microchips have been approved for human implantation.
- Plans are in place to ensure that each and every person in the US will have an electronic health record.
- Advanced face recognition systems are being integrated into CCTV cameras.
- High-powered microphones and loudspeakers are also being attached to CCTV cameras, as the deployment of CCTV surveillance systems rapidly increases and their surveillance capabilities expand.
- DNA databases are rapidly growing and DNA analysis can reveal limitless amounts of information about a person.
- Children are increasingly being digitally fingerprinted and tracked at school.

---

[3] McCullagh, Declan. and Anne Broache "FBI taps cell phone mic as eavesdropping tool" (CNET News, 1 December 2006), available at: http://news.cnet.com/2100-1029-6140191.html

- Corporations are not only retaining vast amounts of data regarding their customers, but are also providing governments with access to their databases.
- Companies are engaged in the vast data mining of online activities and information, and online social media networking websites can track Internet surfing habits.
- ‘Fusion Centers’ and data centers capable of enabling “total information awareness” have been established in the US, As governments are expanding their surveillance and intelligence gathering authority and activities.
- Stories of Western governments conducting surveillance of private electronic communications (emails, etc.) are now commonplace.
- Body scanners capable of seeing beneath clothes are being deployed at airports around the world.
- Devices capable of enabling the user to see through walls are being developed and deployed.
- UAVs, with built-in advanced cameras, are being deployed for domestic surveillance, and law enforcement agencies are increasingly calling for their widespread use.
- Neurotechnologies may one day be capable of being used for reading our thoughts.
- Devices are being developed that are capable of recording and storing video of an entire human life.

While the above list of privacy threats/issues is certainly far from exhaustive, they involve the unprecedented development/deployment of advanced technologies, systems and infrastructures that are highly capable of being used to violate an individual’s right to privacy and pose the newest, and arguably one of the most serious, threats to liberty in modern Western society. Governments, businesses and consumers/citizens increasingly seek to take advantage of the apparent public security/safety, health, social, environmental, commercial and other societal benefits these technologies offer. But, at the same time, governments and businesses (i.e. those who can control the development/deployment of technology) must also sufficiently aim to minimize the privacy threats and societal implications of the widespread advancement, deployment and use of these technologies.

1.2 CENTRAL THESIS

Backed by case studies and overall analysis, the thesis of this dissertation[4] is centered on the general underlying problem that technology is evolving faster than the laws that aim to regulate their use and, as a consequence; the laws are behind the advancement of technology. With the rapid advancement of technology or the inertia of technological development, the current laws and regulation strategies/approaches are increasingly becoming outdated and there is potentially no end in sight. One reason is that lawmaking is normally a gradual process and is primarily reactive, rather than proactive. In addition, the focus is all too often on the implications of the use of technologies, as opposed to the implications of the development of the technologies in the first place.

Privacy/data protection laws are essentially a perfect case in point. The current legal framework, pertaining to privacy/data protection in the US and the UK/EU, focuses predominantly on data controllers/processors, service providers and operators, and traditional policy or legal-based solutions, for the sake of privacy, are mainly focused on the users of privacy-invading technologies, as opposed to the developers/manufacturers. Hence, the Privacy Act 1974 and the Directive 95/46/EC do not apply to the developers/manufacturers of privacy-invading technologies (PITs) or ICTs. This approach may diminish or deter the unlawful or illegitimate use of these technologies, but it may also fail to address the privacy-intrusiveness of the technologies concerned at the design stage. Often, current attempts to regulate the privacy-intrusiveness of the technologies concerned are based on limited technical solutions "bolted on" after a public outcry or significant privacy breach. But, it seems that without robust and comprehensive technical solutions for implementing the principles of privacy, the relevant privacy/data protection laws are increasingly ineffectual.

As this dissertation aims to demonstrate, the law should move away from focusing primarily on data controllers and users/operators of privacy-invading technologies/ICTs and should instead impose technical/design obligations, known as "privacy by design" (PBD) requirements, on the manufacturers/developers. The *concept* of PBD and the PBD requirements should also be technologically neutral (as much as possible). Demonstrated through case studies, the premise is that privacy laws, directly applied to the manufactur-

[4] An overall condensed version of this dissertation was published as an academic paper. see *Privacy by Design & Privacy-Invading Technologies: Safeguarding Privacy, Liberty and Security in the 21st Century* (Legisprudence, Volume 5, Issue 3, Hart Publishing, Oxford, 2012), pp. 297-329.
In addition, a forthcoming academic paper, which focuses on the dissertation's discussion on the challenges, limitations and criticism of Privacy by Design, is to be published in 2012. The foreseen reference is the following: Klitou, D. *A solution, but not a panacea for defending privacy: The challenges, criticism and limitations of Privacy by Design*, Annual Privacy Forum 2012 proceedings (Lecture Notes in Computer Science, Springer-Verlag, 2012).

ers/developers and the design/development of PITs, can more effectively protect privacy against the threats posed by existing technologies and also have, at the same time, a better chance of staying apace with the ever-increasing technological threats to privacy posed by future and emerging technologies. Privacy/data protection laws only applied to data controllers and users/operators of privacy-invading technologies/ICTs are constantly and increasingly falling behind new technological developments.

Although there are standards and legal requirements with regards to data security and audit mechanisms thereof, the other principles of privacy are generally left out. The technical emphasis, at present, found both in law and industry standards, is all too often focused on data security alone. While existing laws may ultimately have an indirect effect on the manufacturers (e.g. data controllers can put pressure on ICT manufacturers to develop privacy-friendly technologies), this has evidently proved insufficient.

This dissertation attempts to address both the general underlying problem and specific threats to privacy and civil liberties in the US and UK, posed by the latest and evermore evolving privacy-intrusive technologies. In doing so, the dissertation also offers some potential solutions, both legal/policy and technologically/architecturally-orientated, to address the privacy threats and current legal dilemmas and to provide some answers to the key research questions (see: section 1.3).

Essentially, the dissertation shows how and why laws that focus on the design/development of PITs may better ensure the protection of privacy and better ensure that the legal framework remains more up-to-date than laws only applied to data controllers/users. The premise is supported and demonstrated through case studies (see: PART II, Chapters 5, 6 and 7). Furthermore, the dissertation overall attempts to show how laws/regulations that mandate the implementation of PBD could potentially serve as a viable approach for *collectively* safeguarding privacy, liberty and security in the 21st Century (see: PART III, Chapters 9 and 10, for further information). However, while the dissertation clearly advocates for the implementation of PBD, it does not ignore the fact that the PBD approach has its own shortfalls and is not a panacea for all issues related to privacy intrusion (see: sections 9.11, 9.12 and 10.19).

It is important to note that the premise of the dissertation was only developed after the legal analysis and assessment of the case studies was completed; during which it was consistently determined or revealed that technical/design solutions (i.e. PBD solutions) could play a more important role than traditional legal solutions for regulating PITs. This determination was not planned or deliberate at all, which explains why the concept of PBD is not clearly or specifically integrated or discussed in most of the chapters.

The dissertation focuses on the following four privacy-invading technologies (PITs) as case studies:

- Body scanners;
- Public space CCTV microphones;
- Public space CCTV loudspeakers; and
- Human-implantable microchips (RFID implants/GPS implants)

Furthermore, as demonstrated through the case studies, the dissertation also argues that both privacy and other civil liberties, on the one hand, and (public/national) security, on the other, can be safeguarded.

1.3 RATIONALE BEHIND THE SELECTION OF THE CASE STUDIES

Some technologies may be regarded as the 'black swans' of PITs, i.e. those technologies that immediately stand out due to their disruptive or controversial and highly-intrusive capabilities and due to their immense societal impacts.[5] This dissertation will focus especially on some of the foremost threats to privacy posed by the following PITs, which are considered to be ´black swans': Human-implantable microchips (RFID/GPS implants); Body scanners; and public space CCTV microphones and CCTV loudspeakers.

Without adequate safeguards, these technologies, and the associated acts of widespread human tracking, full body scanning, audio recording and disturbing people's 'right to be left alone' out in public, could arguably pose some of the most serious technological threats to privacy and liberty in the early 21st Century. Therefore, these technologies require further scrutiny and deserve attention from lawmakers/policy makers in the very near future.

These specific PITs were chosen as the case studies for this dissertation, as a result of the controversy surrounding their increasing deployment and use, their novelty, their highly-intrusive capabilities, the various apparent legal challenges to regulate and/or curtail the associated novel privacy-intrusive capabilities, and the lack of substantial study regarding their escalating development, deployment and use.

The current focus on the privacy concerns of social networking sites, and other online/digital services, has generally ignored the fact that body scanners have rendered clothes obsolete, RFID potentially enables every object or person to be identified and tracked, the integration of microphones with CCTV cameras enables conversations out

---

[5] Nassim Nicholas Taleb equally used the term "black swan" to refer to highly-improbable events that are unpredictable and have an immense impact on society, but their occurrence is believed to be more predictable and less random than they really are. see Taleb, Nassim Nicholas. *The Black Swan: The Impact of the Highly-Improbable* (Random House, 2007)..

in public to be recorded, and CCTV loudspeakers provide CCTV camera operators the immense ability to disturb or scold individuals from afar. The radical privacy-intrusive capabilities of these selected PITs and their enormous potential for abuse or their 'function creep' propensity are resulting in unprecedented intrusions into both our private and public space, threatening not just the right to privacy, but other civil rights and our freedom and personal dignity overall.

It may be argued that body scanners, public space CCTV microphones and CCTV loudspeakers and RFID implants were foreseen. For example, the concept of "x-ray specs" or "x-ray glasses", allowing the wearer to see through objects or clothes, was envisioned decades ago. In addition, George Orwell, in his book *Nineteen Eighty-Four*, conceptualized "telecreens" (two-way screens complete with microphones and loudspeakers), which surrounded the masses, in order to monitor and control their behavior in public spaces. These PITs, therefore, could also be deemed 'black swans', if looked at from Taleb's viewpoint,[6] since their deployment now seems quite predictable, but in actual fact their development and deployment depended on various unpredictable events occurring. For example, the widespread deployment of body scanners in the US depended on the occurrence of 9/11 and the "Christmas Day attack", which were essentially both unpredictable, regardless of the different apparently "obvious" explanations developed subsequently.

In addition, the selected PITs offer potentially significant (public/national) security benefits, which cannot be overlooked. Indeed, body scanners and public space CCTV microphones and CCTV loudspeakers are primarily used by law enforcement agencies. Therefore, by addressing or minimizing the threats to privacy and liberty posed by these PITs, we are facilitating their deployment and public acceptance and, as a result, also potentially helping to safeguard (public/national) security.

PITs mainly concern either the public sphere or the private sphere. The choice of PITs also allows the dissertation to cover both spheres (see Chapter 4 for further explanation). With regards to the private sphere, the changing level of privacy we enjoy over our bodies is explained, with the deployment and use of body scanners as the case study. With regards to the public sphere, the changing nature of the public space and level of privacy we enjoy in public is explained, with the deployment and use of public space CCTV microphones and CCTV loudspeakers in the UK as the case studies. Human-implantable microchips (RFID/GPS implants) concern both the private and public sphere, since HIMs and the corresponding infrastructure impact the nature of the

6 Ibid.

public space and of the human body, and radically change the level of privacy enjoyed in both spheres.

The US and the UK were chosen as the country case studies or legal jurisdictions, on the grounds of actual technological threats and since it is where the chosen PITs are largely being deployed. Both the US and UK needed to be covered, since body scanners and HIMs are predominantly being deployed in the US, while public CCTV microphones and CCTV loudspeakers are predominantly being deployed in the UK. The UK is leading the way in the deployment of CCTV public surveillance systems. For example, London's so-called "ring of steel" has served as a model for New York City's CCTV public surveillance system (Cannataci, 2010).

Moreover, the US and the UK were selected as the country case studies, since both countries are also leading the way in the establishment of a 'surveillance society'. Privacy International, a watchdog on surveillance and privacy, for their 2007 International Privacy Ranking, gave the UK and the US a final score of 1.4 and 1.5 respectively (out of a score range of 1-5, with 1 indicating a surveillance society and 5 indicating a society where privacy is ideally upheld). The final scores of the US and UK were practically equal to the final score of China with 1.3.[7] The UK, in particular, had the lowest score in the EU and, as the UK Government moves to monitor all online activities,[8] this score should be even lower. The UK already has millions of public space CCTV cameras deployed and operating, and the UK's former Information Commissioner, Richard Thomas, himself is well-known for often declaring that the UK is "sleepwalking into a surveillance society". As the leader in the overall development and deployment of PITs, the US is certainly not far behind.

The focus on both the US and the UK also allows for a broader audience. Since the UK is an EU Member State, there is also an opportunity to briefly show some of the differences between the US sectoral approach and the current EU comprehensive approach to privacy protection and to take into account legal precedent of the European Court of Human Rights (ECtHR), where necessary.

7 Privacy International, 2007 International Privacy Ranking, 28/12/2007, available at: http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559597

8 see "Internet activity 'to be monitored' under new laws" (The Telegraph, 1 April 2012), available at: http://www.telegraph.co.uk/technology/news/9179087/Internet-activity-to-be-monitored-under-new-laws.html

1.4 KEY RESEARCH/EVALUATION QUESTIONS

The following are the general underlying research/evaluation questions the dissertation aims to broadly address:

- What changes to society are brought about by the increasing advancement and deployment of the most intrusive PITs?
- How will the latest PITs impact the right to privacy and other civil liberties?
- How can the right to privacy and other civil liberties be ensured?
- What are the main limitations of the right to privacy and/or data protection laws?
- Should new laws be adopted or can existing laws be applied to the new challenges and threats posed by the latest PITs?
- Are the existing fundamental principles of privacy still relevant? If so, how can we uphold the principles of privacy, in light of the threats and challenges posed by the latest PITs?
- How can both security and the right to privacy and other civil liberties be ensured/ safeguarded (in practice and in theory) for the 21st Century?

The following are some of the specific questions addressed:

Body scanners

- In what way is the use of body scanners legal and illegal?
- How should the use of body scanners be regulated to ensure the right to privacy and freedom from unreasonable search and seizure?
- How can both privacy and the effectiveness of body scanners in airport security screening be maintained?
- Are there viable alternatives?

Public space CCTV microphones and loudspeakers

- How does the use of public space CCTV microphones and loudspeakers involve the right to privacy and privacy laws?
- How can the deployment and use of CCTV microphones and loudspeakers be regulated?

Human-implantable microchips (RFID/GPS implants)

- In what way human-implantable microchips (HIMs) alter the nature of the human body?
- To what extent, are RFID/GPS implants a threat to privacy, liberty and human dignity?
- Should RFID/GPS implants be banned? If not, how should RFID/GPS implants then be regulated? What amendments and additions in the legal framework must occur in order to adequately regulate RFID/GPS implants and defend the right to privacy/data protection and other civil liberties?
- When is the tracking of individuals legitimate and illegitimate? When is the use of RFID/GPS implants to identify and track people legitimate and illegitimate?
- Can the government potentially force prisoners or criminals to be implanted? Does the government have the right to order citizens to be implanted for identification purposes? Do employers have the right to dismiss an employee who has refused to be implanted for access control purposes? Should parents be allowed to impose RFID/GPS implants on their minor children?
- When is location information (generated by HIMs) personal information? What is the expectation of privacy for location information?
- Should the criteria of a "reasonable expectation of privacy" and determination of a privacy intrusion be revised?
- How are the private space and public space and the physical world and virtual world potentially merging? What approach can accommodate for this potential merger?

1.5 RESEARCH OBJECTIVES

The overall research goals of the dissertation are:

- To evaluate/assess the legal framework for the protection of privacy in the US and UK (EU) in light of the latest PITs;
- To identify and recommend suitable enhancements, amendments and additions to the US and UK (EU) legal frameworks for the protection of privacy, taking into account the development and deployment of the latest PITs;
- To define an approach for striking a balance between privacy and other civil liberties, on the one hand, and security, on the other.

1.6 RESEARCH METHODOLOGY AND APPROACH

The dissertation somewhat attempts to take a multi-disciplinary approach, with the aim of bringing together several different fields, including law, human rights, international relations, social science, political science and computer science. But, the dissertation generally avoids the social and moral criticism of the rapid development and deployment of PITs. Without arguing against the deployment of PITs, the dissertation instead aims to focus primarily on addressing the legal issues at hand and on proposing practical solutions for ensuring that privacy/liberty is upheld.

For each PIT this dissertation specifically addresses as case studies, their privacy-intrusive capabilities, based on ordinary desk research, are explained and described. Then, the relevant statutory laws, regulations and case law on privacy protection, within either the US or the UK, of special relevance to each of these PITs, are identified and outlined. The case studies for this dissertation specifically include: human implantable microchips (GPS/RFID implants); body scanners; and public space CCTV camera microphones and loudspeakers.

In order to achieve the research objectives and address the key research questions, the adequacy of the legal frameworks of the US and the UK is assessed, in light of the identified intrusive capabilities of the four latest PITs, specifically addressed as case studies. The assessment of the adequacy, and ensuing determination of the deficiencies and dilemmas of the US and UK legal frameworks, is based on the criteria outlined and defined in Chapter 3. The criteria are based on the fundamental principles of privacy and other legal principles/requirements. The policy recommendations on enhancing the legal frameworks, in light of the privacy-intrusive capabilities of each PIT, are subsequently formulated, equally based on the fundamental principles of privacy and the identified legal deficiencies and dilemmas. For body scanners and human-implantable microchips, the US legal framework is evaluated. For CCTV microphones and CCTV loudspeakers, the UK/EU legal framework is evaluated.

The same criteria are used for each PIT for assessing the legal frameworks, in terms of privacy protection, and for determining the required solutions, amendments and additions to enhance the legal frameworks. However, the layout for the separate chapters covering each PIT is not identical, given that the overall privacy implications, intrusive capabilities, circumstances and potential solutions/recommendations that need to be considered, concerning the use and deployment of each PIT, are different.

The problems, root causes, objectives, recommendations and countermeasures addressed by this dissertation are mapped out and summarized in an *A3 Report*[9] (see: Annex I). It is important to note that the A3 Report was developed only after the overall research findings and conclusions were established. Moreover, the overall conclusions and overall policy recommendations of the dissertation (see: Chapter 10) are based on the specific analysis and conclusions/results of the case studies.

The dissertation attempts to take a balanced approach, in order to avoid any extreme or one-sided points of view. Moreover, in order to adopt a more balanced and scientific approach, the different points of view of a variety of stakeholders are thus taken into consideration. While the (potential) threats to privacy and other civil liberties posed by the latest PITs are emphasized, the (potential) societal and security benefits of these PITs are also pointed out.

The research formally began September 2007. Timing is critical for this dissertation, as the world, in terms of technological, policy, legal and political developments, is constantly evolving. The current state of the legal framework in the US and UK, the current state of art of the technologies addressed, and the current situation and circumstances surrounding the deployment and use of these technologies is outlined and evaluated based on the current state of affairs up until *January 2010*, for the most part. However, while the cut-off date is January 2010, there are some exceptions, where necessary or helpful. Indeed, since early 2010, there have been a number of legal/policy developments in the US that are relevant for the dissertation and cannot be ignored. For example, concerning GPS tracking, the US Supreme Court granted a writ of certiorari in the case *US v. Jones* and then later issued a ruling on the legality of the installation and use a GPS tracking device without a warrant. In addition, the EC issued an official draft of their proposed EU General Data Protection Regulation.[10] Also, the FTC published the acclaimed December 2010 Staff Report, "Protecting Consumer Privacy in an

9 An A3 Report, named after the paper size standard on which it is meant to fit on, is an effective method of communicating a chain of reasoning and mapping out thoughts for solving problems. A3 Reports have been extensively used by Toyota Motor Corp. to understand and communicate the root cause(s) of a problem and its solutions. A3 Reports are composed of a sequence of text boxes, which, normally in the following order: (1) identify and explain the problem(s) or issue(s); (2) breakdown the current conditions and reasons (cause and effect) for the problem or issue in order to get to its root cause by asking 5 or more 'Whys'; (3) determine the countermeasures to solve the problem; (4) establish an action plan; (5) identify the desired outcome; (6) implement the plan and follow up. The "5 Whys" technique was developed by Sakichi Toyoda and later adopted by Toyota Motor Corp.

10 see Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11/4 draft.

Era of Rapid Change", which emphasizes the role of privacy by design.[11] Some of these more recent developments will be discussed, albeit in a limited way. Still, the dissertation *generally* does not incorporate additional developments after January 2010, unless where and when deemed required.

1.7 MAIN SOURCES OF INFORMATION

The main sources of information for this dissertation include at least: relevant books and published/academic papers; statutory laws, regulations, and case law; corporate privacy policies and self-regulations; commissioned privacy reports; policy papers; company websites; press releases; current events; news articles; expert views/judgment; stakeholder perspectives; surveys; public consultations; workshop/working group discussions; and conference papers.

1.8 ADDED VALUE

The research predominantly serves to determine if the legal framework for the protection of privacy/personal data in the US and UK is still effective and adequate in light of the deployment of the latest PITs. Diverging from traditional legal dogma pertaining to privacy/data protection in the US and UK, the deficiencies and dilemmas of the respective legal frameworks, particularly concerning the four specific PITs addressed (body scanners, CCTV loudspeakers, CCTV microphones and RFID/GPS implants) are identified. From there, the research proposes recommendations, which include a mixture of new laws and policies, amendments to existing laws, legal definitions and interpretations, privacy safeguards and technological solutions, in order to address the current legal issues and minimize the threats to privacy posed by these latest PITs. Overall, regardless of the PIT in question, the research aims to identify what is required in order to balance the perceived security gains of PITs with the right to privacy and other civil liberties these technologies threaten.

It is further important to note, however, that the recommended legal methods, solutions, definitions and safeguards are written, for the most part, in the form of policy-orientated proposals/recommendations, which are meant to be specific, practical and actionable. These proposals should arguably be considered, in order to enhance the

[11] As a follow-up to the preliminary FTC Staff Report, the FTC Final Report, "Protecting Consumer Privacy in an Era of Rapid Change", was published in March 2012, available at: http://ftc.gov/os/2012/03/120326privacyreport.pdf.

legal framework. However, while these recommendations should be considered for amending existing legislation or drafting new laws, for example, they are not written in a legislative text format, nor are equally comprehensive or technical. Moreover, while this dissertation explores the relevant legal questions and attempts to address these questions, the answers are not all complete, as some of the critical legal questions still need to be left to the courts and lawmakers to decide upon.

1.9 ISSUES AND AREAS NOT SUBSTANTIALLY ADDRESSED

Due to the limited scope of the research, this dissertation specifically does not attempt to formulate comprehensive, specific and widely agreed upon definitions of privacy and liberty. The research neither aims to substantially compare the American and European legal approaches to privacy protection for each case study or analyze the different relationships between the legislative and judicial branches of government. Besides, CCTV microphones and loudspeakers are primarily being deployed and used in the UK, while body scanners and RFID implants are primarily available in the US. In addition, the dissertation does not intend to resolve the long-standing legal debate on technological neutrality or to substantiality add to the broad discussion on the advantages and disadvantages of technological neutrality. Finally, the dissertation does not include substantial discussion on the overall social developments/implications surrounding the ever-increasing deployment of PITs.

1.10 STRUCTURE OF THE DISSERTATION AND OVERVIEW BY CHAPTER

The dissertation is divided into four Parts:

- In PART I, Chapter 2 briefly explains what is meant by privacy, liberty and security, and how they are interrelated. Chapter 3 delineates the assessment criteria this dissertation applies to assess the adequacy of a legal framework in terms of protecting privacy.

- In PART II, Chapter 4 explains what is meant by privacy-invading technologies/ privacy-intrusive technologies (PITs) and how PITs are altering the level of privacy we should expect in the private and public sphere, and provides an overview of technologies that may pose a significant threat to privacy/liberty. Beginning with the first case study of dissertation study, Chapter 5, addresses the implications of the deployment and use of body scanners. For the second and third case studies, Chapter 6 addresses the implications of the deployment and use of CCTV microphones and CCTV loudspeakers. For the fourth and final case study, Chapter 7 addresses the implications of the deployment and use of human-implantable microchips (RFID/GPS implants). Altogether, PART II explains how body scanners should be considered as a strip search by *other means,*[12] how public space CCTV microphones and CCTV loudspeakers can act as the ears and mouth of 'Big Brother', and how HIMs could seriously threaten privacy and alter the way we perceive our bodies as transmitters of information in a location-aware world. Chapter 8 sums up some of the conclusions derived from Part II.

- In PART III, Chapter 9 provides an overview of what is meant by "privacy by design" and an overview of the issues surrounding the concept.

- In Part IV, Chapter 10 concludes with the dissertation's overall research findings, conclusions and policy recommendations, based on the results and analysis of the case studies, and a concise overview of some of the answers to the general research/evaluation questions.

In the Annexes, Annex I contains an *A3 Report*, mapping out and summarizing the central thesis of the dissertation. Annex II contains a summary table with a short overview of the intrusive capabilities of the specific PITs addressed and the corresponding most relevant laws and self-regulations, legal deficiencies, and proposed key recommended legal and technological solutions.

[12] see Saletan, William. "Naked Came The Passenger" (Washington Post, 4 March 2007), available at: http://www.washingtonpost.com/wp-dyn/content/article/2007/03/02/AR2007030202035_pf.html

2 Privacy, liberty & security

2.1 CHAPTER INTRODUCTION

Privacy, liberty and security are important, inter-related concepts that have been debated for centuries.

Section 2.2 outlines the concept of privacy. Section 2.3 provides an overview of the international legal instruments that stipulate the right to privacy. Section 2.4 explains briefly the merits of privacy. Section 2.5 outlines the concept of liberty. Section 2.6 clarifies the relationship between privacy and liberty. Section 2.7 outlines the concept of security. Section 2.8 concludes the chapter with an explanation of the interlinkages between privacy, liberty and security.

2.2 THE CONCEPT OF PRIVACY

Again, it is not the intention of this dissertation to attempt to formulate a comprehensive, specific and widely agreed upon definition of privacy. Instead, the dissertation focuses on assessing the existing legal frameworks, in light of the latest PITs, and on presenting practical, legal and technical measures to safeguard privacy/liberty. Moreover, this dissertation does not focus on conclusively defining the concept of privacy, since such an endeavor is not feasible for a dissertation alone, due to the vast array of different theories and conceptualizations of privacy and conflicting opinions. As Wacks notably once argued, "the long search for a definition of 'privacy' has produced a continuing debate that is often sterile and, ultimately, futile" (1980, p. 10).[13] Even the ECtHR, as Taylor points out, "has never sought to give a conclusive definition of privacy, considering it neither necessary nor desirable" (2002a, p.76). Other legal scholars (e.g. Solove, 2006) have also observed the difficulty and ineffectiveness of trying to conclu-

[13] For further discussion, see Taylor, Nick. *State Surveillance and the Right to Privacy* (Surveillance & Society 1, 2002a), pp. 66-85.

sively and comprehensively define privacy. However, it did not take long to discover that privacy is so difficult to define. Sir James Fitzjames Stephen, more than a century ago, argued "[t]o define the province of privacy distinctly is impossible, but it can be described in general terms" (1873, p. 160).

It may be fair to presume that this enduring futility or difficulty of reaching a comprehensive and determined consensus on the definition of privacy (i.e. what fully constitutes privacy, what constitutes a privacy violation, what merits privacy protection) is the result of the concept's "inherent flexibility"[14] and the significant differences of opinion among legal practitioners/legal scholars and between different generations. For instance, Generation X may overall have a different opinion about privacy and its importance/value than Generation Y (or the "Millennial Generation"). Moreover, the need to take into consideration the current/changing social norms/values, public opinions, ideological trends, available technologies, political circumstances and overall state of affairs (e.g. an extraordinarily high violent crime rate or the aftermath of a terrorist attack) make it even more difficult to broadly/comprehensively define privacy in a fixed and definitive way. The concept of privacy and the belief in its importance/value may also differ among people based on their personalities, personal experiences, interests and more particularly on their occupation and position/role within society. The escalating advancement, deployment and use of PITs have also added to this uncertainty and the difficulty in defining privacy (see section 4.2 for the dissertation's definition of PITs). For example, it may be especially more difficult to define privacy in a high-tech "surveillance society" or within a "ubiquitous information society". Therefore, it should come as no surprise that a consensus on the definition of privacy has yet to be achieved, and the notion of doing so will only become more complicated in the future as technologies continuously advance and social values potentially change. Nevertheless, *the underlying concept of privacy*, which serves as the basis of this dissertation, should be somewhat outlined.

At first, the right to privacy was largely viewed, in US courts, as a defense against any "unreasonable" physical intrusion upon one's private home, private papers, personal belongings and person (i.e. body), strictly in accordance with the Fourth Amendment of the US Constitution. The focal point of the concept of privacy and its legal interpretations, however, has gradually evolved over time, beyond those domains, as modern technology and society has evolved. For starters, as widely recognized, Warren and Brandeis (1890) brought a new focus on the autonomy and seclusion components of privacy, in the wake of the increase in newspapers and photographs, made possible

[14] Feldman, Noah. "Strip-Search Case Reflects Death of American Privacy" (Bloomberg, 9 April 2012), available at: http://www.bloomberg.com/news/2012-04-08/strip-search-case-reflects-death-of-american-privacy.html

by printing technologies and the first cameras (Schermer, 2007), and famously characterized privacy as the right "to be let alone" (Warren and Brandeis, 1890, p. 193). With the rapidly growing use of telephones, the focus of privacy evolved to the privacy of telecommunications. The gradual increase in the use of information technologies/electronic data systems led to the focus on the privacy of personal data stored on computer databases – 'information privacy'.[15] Accordingly, Westin notably defined privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated" (Westin, 1967, p. 7). As questions arose on the morality and legality of abortion and the means employed, the focus of privacy further evolved to personal autonomy/self-determination and the right of individuals to make decisions concerning their own bodies and/or domestic matters. As the advancement, deployment and use of public surveillance CCTV cameras has rapidly increased, and the development of other technologies capable of mass surveillance advances, the right to be left alone has been re-emphasized. The advancement and use of location-tracking devices, location-based services and mobile phones capable of being tracked has led to the focus on 'location privacy' and the privacy of location information. It has also re-initiated a debate on the level of privacy that may (or may not) exist out in public. As the use of e-mail, online social networking (Facebook, etc.), micro-blogging (i.e. Twitter) and e-commerce websites (Amazon, eBay, etc.) continue to increase, the focus of privacy has also swiftly evolved to further address the confidentiality of online (and related offline) activities and initiated the debate on how the 'right to be left alone' could be extended to the information society. As electronic voting machines surfaced and their deployment and use during elections increased, and the potential for the implementation of Internet voting also increases, privacy has also re-focused on the importance of the sanctity of the vote in a democratic society. As electronic health records rapidly increase, the focus of privacy further emphasized the confidentiality of personal medical data. As neurotechnology advances and its applications increase, a new focus of privacy will likely evolve to address the privacy of the mind/brain.[16] As the immense potential of DNA analysis emerged and the use of biometric data increased, the focus of privacy has evolved even further to the privacy of the body (or bodily/corporeal privacy). However, while the concept and focus (i.e. focal point) of privacy is continuously evolving and varies from time to time as technology and society

[15] For the purposes of this dissertation, 'information privacy' is synonymous with 'data protection'.

[16] see "Clive Thompson on Why the Next Civil Rights Battle Will Be Over the Mind" (Wired, 24 March, 2008), available at: http://www.wired.com/techbiz/people/magazine/16-04/st_thompson

evolves, what was previously considered applicable continues to remain relevant, since all of these technologies are still heavily in use.

Privacy, therefore, is not just simply an issue concerning the inviolability of one's private home, private papers, etc. or what is done with one's personal data.[17] For the *underlying and particular purposes of this dissertation*, an understanding of privacy includes the inviolability of a person's mind and body (unless lawfully authorized), the protection of the confidentiality of personal data, the 'right to be left alone', the 'reasonable' confidentiality of communications between two or more people no matter where, how and in what form they occur, and the freedom from undue, unlawful or unreasonable surveillance, whether in public or private places.[18]

The 'right to be left alone' is associated with the freedom from unreasonable, unlawful or disproportionate surveillance and also the right to be free from unnecessary or excessive disturbance, which can interfere with a person's life. This component of privacy, for example, has likely supported the establishment of the National Do Not Call Registry (McClurg, 1995) and the adoption of the Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 in the US, which regulates spam e-mail, and in the EU the relevant provisions of Directive 2002/58/EC, which prohibits unsolicited communications in the form of automatic calls or e-mails. The right to privacy and/or the right to be left alone also supported the creation of anti-stalking laws (McClurg, 1995).

Based on Article 2 of EU Directive 95/46/EC, personal data (or personal information) is "any information relating to an identified or identifiable natural person ('data subject')". As Article 2 (a) states:

> An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity is regarded as information that can be used to directly or indirectly identify an individual.[19]

Personal data normally includes, for instance, a name, address, date of birth, identification number, etc. However, personal information of a far more sensitive character, *for*

[17] For further discussion on the scope of privacy, see, e.g., Nissenbaum, Helen. *Privacy as Contextual Integrity* (Washington Law Review, Vol. 79, No. 1, 2004), pp. 101-140.

[18] see *Ibid*.

[19] see Article 2 (a) of Directive 95/46/EC.

the underlying purposes of this dissertation, includes a person's consumer habits, daily movements, private affairs and activities, voting records, conversations, interactions, images, medical history, DNA, and financial data. This list is also certainly not exhaustive.

It is also difficult to comprehensively define a violation of privacy, since there are so many different types of violations. Instead of trying to provide a single meaning to privacy violations, Solove developed a 'taxonomy of privacy', classifying the range of privacy violations within four basic groups: information collection; information processing; information dissemination; and invasion; and 16 subgroups: surveillance; interrogation; aggregation; identification; insecurity; secondary use; exclusion; breach of confidentiality; disclosure; exposure; increased accessibility; blackmail; appropriation; distortion; intrusion; and decisional interference (Solove, 2006, 2008).

In altering the degree, scope and manner in which privacy is or can be violated, the advancement of technology has also made it more difficult to broadly define what activities constitute a violation of privacy (and what activities do not). For the *underlying and specific purposes* of this dissertation, however, a violation of the right to privacy constitutes any of the following: the unauthorized intrusion upon a person's mind or body; the collection and/or disclosure of an individual's personal data without their consent and/or knowledge and/or without warranted justification; the unlawful (or disproportional/disproportionate) manner in which surveillance is conducted; and the disproportionate interference with the 'right to be left alone'.

2.3 PRIVACY AS AN INTERNATIONAL HUMAN RIGHT

Privacy as a fundamental human right is recognized by diverse, international instruments, such as the Universal Declaration of Human Rights (Art. 12), International Covenant on Civil and Political Rights (Art. 17), European Convention for the Protection of Human Rights and Fundamental Freedoms (Art. 8), Charter of Fundamental Rights of the European Union (Art. 8), American Convention on Human Rights (Art. 11), United Nations Convention on the Rights of the Child (Art. 16), and the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families (Art. 14).

Article 12 of the Universal Declaration of Human Rights (UDHR) declares:

> No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Article 17 of the ICCPR is basically identical to Article 12 of the UDHR.

Article 11 of the American Convention of Human Rights states:

> 1. Everyone has the right to have his honor respected and his dignity recognized.
> 2. No one may be the object of arbitrary or abusive interference with his private life, his family, his home, or his correspondence, or of unlawful attacks on his honor or reputation.
> 3. Everyone has the right to the protection of the law against such interference or attacks.

Article 16 of the Convention on the Rights of the Child states:

> 1. No child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation.
> 2. The child has the right to the protection of the law against such interference or attacks.

Article 14 of the International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families states:

> No migrant worker or member of his or her family shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home, correspondence or other communications, or to unlawful attacks on his or her honour and reputation. Each migrant worker and member of his or her family shall have the right to the protection of the law against such interference or attacks.

Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms states:

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

Article 7 of the Charter of Fundamental Rights of the European Union provides for the right to privacy, and Article 8 explicitly states:

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

2.4 THE MERITS OF PRIVACY

While this dissertation will neither explain or analyze in-depth the merits of privacy, since it focuses instead on regulating the new and specific threats to privacy posed by the latest technologies, those merits should be briefly outlined, in order to highlight why privacy matters and deserves considerable attention, especially as significant ICT industry players are increasingly promoting publicly the contrary perspective.

When comparing each of the international human rights instruments listed above, with the exception of the ECHR, it becomes clear that the right to privacy is explicitly linked with the terms “reputation” and “honor”. While the ECHR does not specifically mention the terms in Article 8, the ECtHR has equally associated privacy with honor and reputation on numerous occasions. Thus, as a result, the right to privacy is clearly recognized as a crucial element for realizing personal dignity and self-respect and the respect deserved from others.

The right to privacy can help to foster personal autonomy (see, e.g., Feldman, 1994) and can help enable individuals to take decisions concerning domestic matters free from excessive or undue government interference (see, e.g., Feldman, 2002). However, privacy is more than just a constraint on a prying government or the freedom from excessive scrutiny of private matters; it is also an essential component for developing our own identities, for realizing who we are as individuals, and for developing/maintaining different types of relationships (Warner, 2005). “Without privacy people might feel inhibited from forming close relationships within the family, or outside in social groups” (Taylor, 2002a, p. 82). “It [privacy] allows the social spheres to function and as a result a degree of privacy helps the community to function” (*Ibid.*). In that sense, privacy is essential for individuals to develop their personality, achieve self-realization, and enjoy intimate relationships and social and emotional well-being. Hence, the lack of privacy could lead to the undesirable conformity of behavior and obstruction of individuality or individualism (Schermer, 2007, p. 73).

2.5 THE CONCEPT OF LIBERTY

Liberty has found its contemporary meaning from the thinkers Locke, Fitzjames Stephen, Hume, Hobbes, Rousseau, Mill and Berlin (Schermer, 2007). Berlin (1958) prominently classified liberty into 'positive liberty' and 'negative liberty'. Positive liberty confers a citizen's *freedom to* exercise their civil rights, while negative liberty confers a citizen's *freedom from* undue government interference in the exercise of their civil rights (Schermer, 2007).

For the *underlying purposes of this dissertation*, liberty is simply the collective term for fundamental civil, political and social rights, in addition to physical liberty. Civil and political rights include, for example, the freedom of speech/expression, freedom of assembly, freedom of movement and the right to privacy, all of which are widely accepted to be necessary for the establishment and preservation of a free and democratic society.

2.6 PRIVACY AND LIBERTY

Privacy and liberty are interrelated and should be protected in an integrated and comprehensive manner.[20] As the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) point out, "the protection of privacy and individual liberties constitutes one of many overlapping legal aspects involved in the processing of data" (para. 29). Privacy is not an end, but rather a means to an end. Instead, the end is greater liberty. In other words, "[p]rivacy is an enabling right; it creates the foundation for other basic entitlements" (Holtzman, 2006, p. 53). For Gavison (1980), privacy also serves to promote liberty and the benefits of a free and democratic society.

The Canada Supreme Court Justice (retired) Hon. Gérard V. La Forest, in *R. v. Dyment*, prominently judged that "privacy is at the heart of liberty in a modern state" and "[t]he restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state".[21] Westin earlier expressed his belief that "a balance that ensures strong citadels of individual and group privacy and limits both disclosure and surveillance is a prerequisite for liberal democratic societies" (Westin, 1967, p. 24). The Closing Communiqué of the 28th International Conference of Data Protection and

20 Hence the reason, for example, why Section 222(a)(5)(A) of the Homeland Security Act requires the DHS Chief Privacy Officer to "coordinate with the Officer for Civil Rights and Civil Liberties to ensure that programs, policies, and procedures involving civil rights, civil liberties, and privacy considerations are addressed in an integrated and comprehensive manner" (emphasis added).

21 *R. v. Dyment* [1988] 2 S.C.R. 417, at 427-8.

Privacy Commissioners (London, 2006) identified that the "protection of citizens' privacy and personal data is vital for any democratic society, on the same level as freedom of the press or the freedom of movement".[22] The Communiqué further added: "Privacy and data protection may, in fact, be as precious as the air we breathe: both are invisible, but when they are no longer available, the effects may be equally disastrous".[23] As the Madrid Declaration warns, "the failure to safeguard privacy jeopardizes associated freedoms, including freedom of expression, freedom of assembly, freedom of access to information, non-discrimination, and ultimately the stability of constitutional democracies".[24]

Privacy also encourages, to a certain degree, the participation of citizens in the overall democratic process, the exercise of freedom of speech/expression, public discourse and the freedom of movement – all of which are necessary in a democratic and free society. For example, privacy: requires the preservation of secret balloting during an election; rejects the calculated attempt to identify participants at a peaceful protest or to expose the identity of bloggers/writers/journalists/users of Twitter/whistleblowers, etc., who wish to remain anonymous while lawfully exercising their freedom of speech; to unduly record private conversations without consent no matter where they occur; and to track people's movements without their permission or due authorization. The coupling of election votes with personal data, the intentional identification of peaceful protestors, the exposure of the identity of writers/journalists/bloggers/users of Twitter/whistleblowers, etc. against their will, the recording of conversations out in public and the constant tracking of people's movements all risk having a 'chilling effect' respectively on the right to vote, the freedom of assembly, the freedom of speech, freedom of the press, the freedom of movement and thus democracy overall. A threat to privacy, therefore, is also a significant threat to liberty, since privacy and liberty indeed go hand in hand.

Privacy, as Schermer points out, is essentially a negative liberty (2007, p. 121), since it is the *freedom from* undue surveillance, scrutiny and observation, and is often categorized as the 'right to be left alone'. If *knowledge is power*, as Sir Francis Bacon famously first aphorized, then the more knowledge someone knows about another person, the more control he/she can exercise over that person (Schermer, 2007, p. 73). Therefore, since privacy is meant to restrict what an individual or other entity may know or discover about another individual, then privacy can serve as a limit or

22 Available at: http://privacy.org.nz/28th-international-conference-of-data-protection-and-privacy-commissioners

23 *Ibid*.

24 Global Privacy Standards for a Global World, The Civil Society Declaration, Madrid, Spain, 3 November 2009, (known as the Madrid Privacy Declaration), available at: http://thepublicvoice.org/madrid-declaration/

constraint on the control governments (or other entities) can exercise over individuals (*Ibid.*). Privacy, on the other hand, is also a positive liberty, since it may endow individuals, for instance, personal autonomy/personal sovereignty, i.e. the *freedom to* take autonomous decisions on their personal/domestic matters (see, e.g., Feldman, 1994).

2.7 THE CONCEPT OF SECURITY

Security is also legally a universal human right.[25] The underlying concept of security is, first and foremost, the protection of persons from injury, harm or termination and, secondly, the protection of objects/property from unlawful/unauthorized damage or destruction. There are various interrelated branches of security and different methods and means of achieving security. In addition to data security,[26] this dissertation predominantly covers public security, aviation security and the security of critical infrastructure (i.e. homeland/national security).

Public security refers to the protection of citizens, which is often a duty of local, regional and national authorities. A variety of threats to public security, for instance, include: murders; armed robberies; kidnappings; deadly virus pandemics; terrorist attacks; and significant natural disasters. Methods and means of helping to maintain public security, for instance, include: the adoption of criminal laws; and the establishment of institutions (e.g. police forces) to enforce the laws and other institutions (e.g. courts) to punish those who violate the law. Other more recent methods and means include the use of technology, such as public surveillance technologies, advanced imaging technologies, forensic technology and ICT infrastructure/applications.

Aviation security refers to the security of airports and aircraft, including the persons onboard, from harm caused by a terrorist attack or hijacking. Aviation security is (primarily) focused on preventing any weapon or explosive device from being brought on board or near an aircraft.[27] Methods and means of achieving aviation security, for instance, include: the screening of passengers and luggage, with the use of technology (metal detectors, X-ray machines, body scanners, etc.) and human resources (i.e. airport security personnel); passenger profiling; and intelligence gathering and analysis.

[25] see, e.g., Charter of Fundamental Rights of the European Union (2000), Article 6.

[26] Data security concerns the security of information technology/infrastructures and the information stored thereof.

[27] Though, in the US, for example, aviation security personnel are also heavily focused on preventing any prohibitive item (e.g., lighters, etc.) from being brought on board.

The security of critical infrastructure is an important sub-branch of national security/homeland security. For the most part, the security of critical infrastructure, for instance, includes the protection of nuclear power plants, the electricity transmission/distribution grid, water reservoirs/treatment plants, dams, bridges, airports, seaports, railways, etc. against a terrorist attack or act of sabotage, including from a cyber attack.[28] Methods and means of achieving the security of critical infrastructure, for instance, include: the deployment of police forces, the national/civil guard and other security personnel; the use of physical access control technology; the methods/means used in intelligence gathering and analysis; and cyber security technological measures and procedures.

2.8 PRIVACY, LIBERTY AND SECURITY

The (individual) rights to privacy and personal liberty are not absolute and must be interfered with for the sake of the 'common good' of society (Etzioni, 1999). Security is, indeed, a common or public good, and privacy and liberty, to a certain extent and under certain conditions, have been sacrificed in the name of security. There are certainly plenty of examples where the liberties of individuals have been limited for the sake of security. Law enforcement and national intelligence agencies, for example, have been granted certain authority to collect vast amounts of personal data and infringe upon the right to privacy, in order to prevent a terrorist attack. Online activities/communications are significantly monitored. Global financial transactions are continuously monitored to discover terrorism financing activities. Mobile phones must be capable of being wiretapped by law enforcement agencies and must be capable of revealing the location of where a call is made. At an airport, a patdown or strip search, conducted in accordance with the law and based on the required level of suspicion, is permitted for the purpose of ensuring the security of commercial aviation. And last, but not least, a person's liberty may be taken away, if they have committed a serious crime or significantly interfered with the liberty of another person. As the Constitution Committee of the UK House of Lords sums up, "[n]ational security, public safety, the prevention and detection of crime, and the control of borders are among the most powerful forces behind the use of a wide range of surveillance techniques and the collection and analysis of large quantities of personal data".[29]

---

[28] Cyber security has become absolutely essential for national security and the security of critical infrastructure.

[29] Constitution Committee - Second Report, Surveillance: Citizens and the State (Session 2008-09), para. 45, available at: http://www.parliament.the-stationery-office.com/pa/ld200809/ldselect/ldconst/18/1802.htm

However, given the important merits, as described in section 2.4, privacy is also a common good. Although the right to privacy and other civil liberties are indeed not absolute, and must always be enforced in relation to the common good/general interest of society as a whole, infringements must also be minimized, as far as possible. Moreover, the measures taken to ensure security, which may limit the exercise/enforcement of the right to privacy/data protection, must be both necessary and relative for achieving legitimate objectives (i.e. subject to the principle of proportionality) or needed to protect the freedoms/rights of others, and the limitations must be provided for by law.[30]

Yet, sometimes privacy can potentially conflict with the needs of security and other civil liberties. For example, terrorists could potentially benefit from the vulnerabilities of patdowns, which may result from the legal requirements of bodily privacy and the principle of proportionality. Online anonymity or the incorporation of encryption technologies (a type of Privacy Enhancing Technology) could potentially enhance the ability of terrorists to communicate undetected and to hide behind data protection. Others have similarly pointed out that online copyright infringers, virus disseminators and "cyber-bullies" can hide behind strong data protection rules, which can negatively affect the value of the freedom of expression.[31]

On the other hand, the protection of privacy can also help to ensure security. For instance, the private communications of heads of state, intelligence agents, ambassadors and other government officials are vital for national security, and any breach of this privacy could be detrimental to national or even international security. This was initially a concern, for example, when the mobile phones of the former Prime Minister of Greece, Costas Karamanlis, and several of his cabinet ministers were wiretapped. The secrecy (i.e. privacy) of national intelligence and the concealment of the identity of intelligence agents are also vital for national security. Moreover, the secrecy of the locations, characteristics and vulnerabilities of critical military bases, particularly of

[30] see, e.g., the Charter of Fundamental Rights of the European Union, Article 52(1).

[31] For example, during the post-i2010 Public Hearing on "Priorities for a new strategy for European Information Society" held 23 September 2009 in Brussels, which I attended, a representative from the Creative and Media Business Alliance (CMBA) made the following oral statement: "Some, such as cyber-squatters, spammers, identity thieves, virus disseminators, cyber-bullies and other illegal content providers call for more "data protection" and "safe harbours" on the Internet in the name of freedom of expression and hide behind these but do not respect them themselves". CMBA's full statement is available at: http://ec.europa.eu/information_society/eeurope/i2010/docs/post_i2010/public_hearing/cmba.pdf

Special Forces, and the suppression of the publication of this information are also vital for national security.[32]

Not only is security considered a universal human right in itself, but security is also equally essential for maintaining privacy and other civil liberties/human rights. Without security, there can be no liberty. As Neocleous (2007) and Waldron (2003) both explain, it is not always a matter of balancing security with liberty and it is mistaken to assume that the relation between security and liberty is self-evidently a zero-sum game. In addition, as Neocleous (2007) points out, key classical and contemporary liberal thinkers, including Adam Smith, Thomas Paine and Michel Foucault, equated the liberty of individuals with the security of individuals. Neocleous (2007) also highlights the significance of how Adam Smith (1776) argued "upon impartial administration of justice depends the liberty of every individual, the sense which he has of his own security".[33] Similarly, as Neocleous (2007) additionally highlights, for William Paley (1785), "the loss of security" leads to "the loss of liberty".[34]

Indeed, security and liberty go hand in hand. For instance, public security is crucial for our physical, social and economic well-being and allows for the conditions of prosperity. Data security, which is the protection against unauthorized access to personal data, is absolutely crucial for realizing the right to privacy/data protection. Aviation security both facilitates and enhances the freedom of movement of people, not to mention that it also facilitates international commerce. Public security and the security of critical infrastructure preserve the right to life and the right to lawfully pursue success and happiness.

There is no denying that without security (i.e. aviation security, national/public security, data security, etc.), life, as we know it, at least in the Western world, would essentially not exist. However, privacy can also assist in the maintenance of security, and privacy and other corresponding civil liberties are significant for the pursuit of happiness. Therefore, any legal framework must equally ensure the preservation of privacy and liberty.

---

32 For example, the recording and recent publication of detailed images of the perimeters of the headquarters of the SAS (British Special Forces) by Google on Street View, including its precise location, has been deemed a serious threat to security by UK military leaders and Members of Parliament. see "Fury as Google puts the SAS's secret base on Street View in 'very serious security breach'" (Daily Mail, 19 March 2010), available at: http://www.dailymail.co.uk/news/article-1259162/Google-Street-View-shows-secret-SAS-base-major-security-breach.html

33 Smith, Adam. *An Inquiry into the Nature and Causes of the Wealth of Nations* (Methuen & Co., Ltd., 1904, 5th edition, first published 1776), v.1.68.

34 Paley, William. *The Principles of Moral and Political Philosophy* (R. Faulder, 1785), pp. 444-45.

Particularly, amid the GWOT in a post-9/11 world, the realization of security and the prevention of a terrorist attack merit the sacrifice of privacy and liberty, albeit to a limited degree and under certain controlled circumstances. The key objective then is to identify and implement a balanced and integrated approach for safeguarding privacy, liberty and security in the 21st Century.

3 Criteria for assessing the adequancy of a legal framework in terms of protecting privacy

3.1 CHAPTER INTRODUCTION

It is important to explain what is meant, throughout this dissertation, by an "adequate" or "inadequate" legal framework in terms of protecting privacy, and on what basis, criteria and guidelines, using which methodology, is a legal framework assessed to determine if it is adequate or inadequate.

Section 3.2 introduces the question of what is meant by an adequate privacy legal framework. Section 3.3 introduces the principles of privacy. Section 3.4 explains the purpose and meaning of each privacy principle. Section 3.5 briefly outlines the differences between the European and American approach to safeguarding the right to privacy/data protection. Section 3.6 outlines additional required characteristics for a legal framework to be considered sound. Section 3.7 briefly lists some measures that should be taken before any relevant law is enacted. Section 3.8 outlines some legal criteria specific to the US, while Section 3.9 outlines some specific criteria specific to the UK. Section 3.10 clarifies how the existing privacy principles still apply.

3.2 AN ADEQUATE PRIVACY LEGAL FRAMEWORK?

As a starting point, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter called "Directive 95/46/EC" or "Data Protection Directive") provides some guidance on determining adequacy and can help to establish a set of criteria for assessing a legal framework in terms of its adequacy in protecting privacy. The Data Protection Directive requires that EU Member States enact laws prohibiting the transfer of personal data to countries outside the EU that fail to ensure an "adequate level of [privacy] protection",[35] with certain derogations. As provided

[35] EU Directive 95/46/EC, Art. 25.

by Article 25(2), when assessing the "adequacy" of the level of privacy protection in a country the following should be considered or looked at:

- the nature of the data;
- the purpose and duration of the proposed processing operation or operations;
- the rules of law, both general and sectoral, in force; and
- the professional rules and security measures complied with.

But, the Data Protection Directive does not explicitly or necessarily specify the substantive criteria for determining the "adequacy" of the legal frameworks of non-EU counties in terms of privacy protection.

In response, the Article 29 Working Party[36] provided further guidance on assessing adequacy in a 1997 document, titled: "First orientations on Transfers of Personal Data to Third Countries – Possible Ways Forward in Assessing Adequacy".[37] However, the Article 29 Working Party predominantly dealt with assessing the adequacy of law in terms of information privacy or data protection, which is essentially not broad or comprehensive enough to assess the overall adequacy of privacy/data protection laws with regards to the growing unique challenges posed by many of the latest PITs. Furthermore, the European Commission more recently also expressed their recognition in the important need to "clarify the Commission's adequacy procedure and better specify the criteria and requirements for assessing the level of data protection in a third country or an international organisation".[38]

---

[36] The Article 29 Working Party is a European advisory body on data protection and privacy established under Directive 95/46/EC.

[37] Discussion document WP4 (5020/97), *First orientations on Transfers of Personal Data to Third Countries — Possible Ways Forward in Assessing Adequacy.*

[38] Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, A comprehensive approach on personal data protection in the European Union, Brussels, 4.11.2010, COM(2010) 609 final (p. 16).

3.3 INTERNATIONAL CONSENSUS IN PRINCIPLE

The principles of privacy/data protection embodied in the Data Protection Directive are clearly based on those previously established by the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) (hereinafter called "OECD Privacy Guidelines"),[39] the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (1981), and the UN General Assembly's Guidelines for the Regulation of Computerized Personal Data Files (1990). The OECD Privacy Guidelines, in particular, have not only significantly served as the basis of domestic privacy laws in Western democratic nations, but have led to further establishing privacy as a recognized international norm.

There is an international consensus over the fundamental privacy principles and basic rules, which are shared among Western democratic nations and serve as the core substance of privacy and/or data protection laws (Bennett, 1992, p. 95).[40] These fundamental privacy principles recur in some shape or form throughout numerous statutory sources of law, whether domestic, regional or international, 'hard' or 'soft', and have constituted as the minimum standard of adequate privacy protection. The fundamental privacy principles apply to both the commercial activities of data controllers and the law enforcement activities of public authorities.

The US Federal Trade Commission (FTC) identifies the following as the five core principles of privacy protection:[41]

(1) Choice/Consent
(2) Access/Participation
(3) Notice/Awareness
(4) Integrity/Security
(5) Enforcement/Redress

While overall the privacy/data protection principles of the FTC, Data Protection Directive (Directive 95/46/EC) and the OECD are similar, the FTC's set of core prin-

---

39 The OECD Privacy Guidelines were based, in part, on the original Fair Information Principles (FIPs), established by the US Department of Health, Education and Welfare in the 1973 report, "Systems, Records, Computers, and the Rights of Citizens". The Privacy Act of 1974 (5 U.S.C. § 552a) also embodies the FIPs for regulating the collection and processing of personal data by federal agencies.

40 For further discussion, see Bennett, Colin J. R*egulating Privacy: Data Protection and Public Policy in Europe and the United States* (Cornell University Press, 1992).

41 Fair Information Practice Principles (FIPPs), available at: http://www.ftc.gov/reports/privacy3/fairinfo.shtm

ciples (or Fair Information Practice Principles (FIPPs))[42] was chosen, since they are arguably more neatly presented and concisely worded. Critically missing, however, from the FTC's set are **(6) the "*purpose specification principle*"**,[43] and **(7) the "*use limitation principle*"**,[44] both of which were formulated in the OECD Privacy Guidelines and are significantly applicable to privacy protection in general. In terminology, missing from both sets is the generally accepted legal **(8) *principle of proportionality***.

Similarly, the eight data protection principles, listed in the Data Protection Act 1998 (DPA),[45] which transposes Directive 95/46/EC into UK domestic law, requires that all personal data must be:

1. Processed fairly and lawfully;
2. Obtained and used only for specified and lawful purposes;
3. Adequate and relevant, and not excessive;
4. Accurate and, where necessary, up to date;
5. Kept no longer than necessary;
6. Processed in accordance with the rights of individuals;
7. Secure; and
8. Transferred only to third-party countries that have adequate data protection laws and practices

These data protection principles are parallel to the principles of privacy selected here. The first data protection principle and the conditions that must be met in accordance with Schedules 2 and 3 of the DPA are parallel to the principle of consent/choice. The second data protection principle is parallel to the purpose specification principle and the use limitation principle. The third data protection principle is parallel to the principles of proportionality and data minimization. The fourth data protection principle is parallel to the access/participation principle and the integrity principle. The fifth data protection principle is parallel to the use limitation principle. The sixth data protection principle is parallel to the principles of notice/awareness and consent/choice. The seventh data protection principle is parallel to the principle of security/integrity.

[42] For instance, the so-called "Bill of Rights" for online privacy, developed with major industry players, is also significantly based on the FIPPs. The FIPPs are rules on the fair treatment of personal data (Schwartz, 2000) and are "the building blocks of modern information privacy law". (Schwartz, 1999, p. 1614).

[43] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980), Art. 9.

[44] *Ibid.*, Art. 10.

[45] Data Protection Act 1998, Schedule 1, Part I.

Altogether, the principles of privacy, with the exception of the principle of consent, also serve as the agreed upon principles between the US and EU for a potential binding transatlantic agreement on the exchange of data for law enforcement purposes and the protection of privacy thereof.[46] The principles of privacy also serve as the basis for the EC's proposal for a new Directive on the processing of personal data for law enforcement purposes.[47]

A wide-ranging and thorough set of criteria permits the clear assessment of the legal adequacy of privacy/data protection laws or lack thereof with regards to the latest PITs. To determine if a legal framework is adequate in terms of protecting privacy and personal data, it should be evaluated against this set of criteria, taking into consideration the intrusive capabilities of PITs (see Chapter 4) on a case-by-case basis.

Throughout this dissertation, the fundamental principles of privacy/data protection will serve, in one way or another, as the criteria and analytical basis for assessing the adequacy of the US and UK legal frameworks/legal practices, with regards to the latest PITs, and for establishing what, if any, amendments, corrections or enhancements to the US and UK legal frameworks are necessary. For the sake of this dissertation, if a legal framework, in its present form, does not fulfill the fundamental privacy principles, where applicable, then it is inadequate (to a certain degree).

3.4 PURPOSE AND MEANING OF EACH PRINCIPLE

The purpose and meaning of each of the interrelated fundamental privacy principles shall correspond to the following:

(1) *Choice/Consent*

The OECD Privacy Guidelines do not specify exactly what constitutes as consent and how to determine consent. The choice/consent principle is also embodied in the *collection limitation principle* in the OECD Guidelines.

---

46 see the Final Report by EU-US High Level Contact Group on information sharing and privacy and personal data protection, May 2008.

47 see Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final, Brussels, 25.1.2012.

To determine consent, several aspects should be considered, including whether the consent is informed (see principle (3) *notice/awareness*), how the consent was obtained by the data controller or granted by the person concerned and whether the consent was somehow forced or if the consent was somehow tied into the permitted exercise of another human right (i.e. indirectly forced). As Article 2 (h) of Directive 95/46/EC requires, consent, in order to be valid, must be "freely given specific and informed". Moreover, consent must be "unambiguous".[48] The Article 29 Data Protection Working Party published an opinion further specifying what constitutes valid consent and clarifying the meaning of "freely given", "specific", "informed" and "unambiguous".[49] According to the Article 29 Working Party, "freely given" implies that the consent is a "real choice" and is not based on deception, intimidation, coercion or the threat of significant negative consequences.[50] "Unambiguous" consent implies that there is "*no doubt* as to the data subject's intention to deliver consent".[51]

Directive 95/46/EC also stipulates that a data subject's consent can be given through any "indication of his wishes". As the Article 29 Working Party clarifies, "[t]here is in principle no limits as to the form consent can take".[52] Consent may include not only "a handwritten signature affixed at the bottom of a paper form, but also oral statements to signify agreement, or a behaviour from which consent can be reasonably concluded".[53] Thus, for the purposes of this dissertation, and in line with Directive 95/46/EC, consent can be validly expressed in written, verbal or electronic form. However, as the Article 29 Working Party also points out, "oral consent may be difficult to prove and, therefore, in practice, data controllers are advised to resort to written consent for evidentiary reasons".[54] In any case, the express authorization must be recorded or documented.

For the purposes of this dissertation, in line with widely accepted notions, consent shall mean a data subject's voluntary, informed and expressed authorization to process his/her personal information or to intrude upon his/her privacy, thereby granting the

[48] see Article 29 Data Protection Working Party, WP187, Opinion 15/2011 on the definition of consent, Adopted on 13 July 2011.

[49] *Ibid*.

[50] *Ibid*., p. 12.

[51] *Ibid*., p. 21.

[52] *Ibid*., p. 11.

[53] *Ibid*.

[54] *Ibid*., p. 25.

person concerned personal autonomy and the freedom to meaningfully choose what he/she would like to reveal about him or herself.

There are certain exceptions to the principle of consent, including when necessary for the protection of public security or for reasons of legitimate public interests, the safety or vital interests of the person concerned (i.e. emergency health concerns), the administration of justice or the prevention or investigation of a criminal offense by competent authorities, in accordance with the law. Consent is also not required when the collection and processing of personal data is deemed necessary to prevent threats to public/national security. Thus, the principle of consent is not applicable for law enforcement operations or surveillance activities, when carried out in accordance with the law, since these activities certainly require secrecy to be effective (Schwartz, 2000).[55] In addition, consent is not required, for obvious reasons, when the processing pertains to personal data that the concerned data subject clearly made public himself/herself (e.g. by publishing it on the Internet via Facebook, Twitter, Blogger, etc.).

With regards to choice/consent, the following are some questions that should be addressed, where applicable:

1. When is consent specifically required and not required?
2. How can consent be expressed? Is the expression of consent recorded/documented?
3. When is consent considered informed and meaningful?
4. When is consent perceived to be given freely and/or non-freely?
5. Are data subjects permitted to change or withdraw their consent?
6. Is consent required each and every time personal data is collected and processed?
7. What are the consequences of refusing?

(2) *Access/Participation*

Access and/or participation, for the purposes of this dissertation, shall refer to a data subject's right of access to the personal data held by data controllers and the capacity or opportunity to review that data and to request that the data be erased or corrected (for instance, where it is evidently determined that the data is inaccurate). Moreover, access/participation encompasses the capacity of data subjects to have removed or the ability

[55] see Schwartz, Paul M. *Beyond Lessig's code for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices* (Wisconsin Law Review, Volume 2000, Issue No. 4, 2000), pp. 743-787, at 784.

to remove themselves any unlawfully retained personal data.[56] The access/participation principle is referred to as the *individual participation principle* in the OECD Guidelines. The expansion of the access/participation principle could also include the right for data subjects to set their 'privacy preferences',[57] where appropriate, feasible and/or technically possible. However, the principle of access/participation may also be limited for law enforcement purposes or national security interests, albeit in accordance with the law.[58]

With regards to access/participation, the following are some questions that should be addressed, where applicable:

1. How accessible is the relevant personal data to the person it concerns?
2. How is the right to access and participate granted or implemented?
3. When can a request for access and/or participation be refused?

(3) *Notice/Awareness*

Notice and/or awareness, as commonly understood, pertains essentially to the requirement of data controllers and/or processors[59] to clearly and/or visibly communicate, for instance, when personal data could be or is being collected, what sort of information could be or is being collected, how that information could be or is being collected (i.e. using which technology, method or means), why (i.e. for which reason(s)) and by whom (i.e. the identity of the data controller/data processor and often their contact information).[60] This awareness will also help data subjects to make an informed choice without which the data subject's consent will not be informed or will be ill-informed. The notice/awareness principle is also based on the *principle of transparency* and is

---

[56] see OECD Privacy Guidelines, Explanatory Memorandum, para. 59; Fair Information Practice Principles, available at: http://www.ftc.gov/reports/privacy3/fairinfo.shtm

[57] Privacy preferences are basically the stipulated circumstances under which a data subject has knowingly given his/her consent for a data controller/data processor to process his/her personal data.

[58] see Article 17 of Council Framework Decision 2008/977/JHA, and Article 13 of Article 17 of Framework Decision 2008/977/JHA, and Article 11 of the EC's proposal for a Directive on the protection of individuals with regard to the processing of personal data for law enforcement purposes, COM(2012) 10 final, Brussels, 25.1.2012.

[59] Article 2 (d) of Directive 95/46/EC defines data controllers as "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data" and paragraph (e) defines a data processor as "a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller".

[60] see OECD Privacy Guidelines, Explanatory Memorandum, para. 57; Fair Information Practice Principles, available at: http://www.ftc.gov/reports/privacy3/fairinfo.shtm

essentially the same as the *openness principle* found in the OECD Privacy Guidelines. Nonetheless, there are also certain exceptions to the notice and/or awareness principle when the exceptions are proportionate and necessary for law enforcement purposes, in accordance with the law, or necessary for competent authorities to execute their legitimate responsibilities.[61]

With regards to notice/awareness, the following are some questions that should be addressed, where applicable:

1. In what form should the notice be communicated?
2. Where is the notice communicated?
3. What is exactly communicated?
4. Who is primarily responsible for ensuring the notice is appropriately visible?

(4) *Integrity/Security*

The security of personal data and of the infrastructure storing that information is at the heart of privacy. Without data security, there can be no data protection/privacy. The security of personal data often corresponds to the requirement of data controllers to take the necessary technical and organizational measures to safeguard against any unlawful or unauthorized access, use, modification or disclosure of any personal data that they are storing.[62] Data security is, therefore, also essential for data integrity and the *data quality principle* of the OECD Privacy Guidelines, which corresponds to the notion of data accuracy, relevance and reliability.[63]

With regards to data integrity/security, the following are some questions that should be addressed, where applicable:

1. What measures must be taken to ensure the integrity and security of personal data?

---

[61] see Article 13 of Directive 95/46/EC; Article 17 of Council Framework Decision 2008/977/JHA; Article 11 of the EC's proposal for a Directive on the protection of individuals with regard to the processing of personal data for law enforcement purposes, COM(2012) 10 final, Brussels, 25.1.2012.

[62] see OECD Privacy Guidelines, Explanatory Memorandum, para. 56; Fair Information Practice Principles, available at: http://www.ftc.gov/reports/privacy3/fairinfo.shtm

[63] The original FIPs, established by the US Department of Health, Education and Welfare, included data "reliability", and the recent Department of Commerce, Internet Policy Task Force Green Paper, "*Commercial Data Privacy and Innovation* in the Internet Economy: A Dynamic Policy Framework" (2010), affirmed that organizations must ensure that stored personal information is "accurate, relevant, timely, and complete" (p. 26).

2. If possible, how can data controllers and data subjects ensure that these measures have been implemented or realized?
3. Are these measures mandated in accordance with binding hard laws /regulations or encouraged through soft laws/voluntary standards/codes of conduct?

(5) *Enforcement/Redress*

Although the privacy principles are inter-dependent and each is equally fundamental, like integrity/security, *enforcement* is crucial. The principles are only genuinely effective to the extent and scope in which they are complied with, implemented or followed in practice. Both the privacy principles and the laws that embody the principles cannot enforce or implement themselves on their own. Essentially, without the means of enforcement, the privacy principles could end up ineffective or even ignored. It is, therefore, necessary to consider not only the content of the law, but also the means of enforcement or the enforcement mechanisms that are in place to ensure the laws have a genuine effect and impact.

Enforcement, for the purposes of this dissertation, entails the impartial means to oversee and verify compliance and investigate and resolve complaints. Accordingly, the principle of enforcement requires independent and effective oversight/supervision. Enforcement also includes the availability of both non-judicial (or administrative) means to provide appropriate redress and judicial means to penalize the responsible parties who violate the right to privacy. Arguably, victims of privacy violations should also have the right to receive damage awards, where deemed appropriate by a court of law. Criminal sanctions should be mandated for serious violations. Arguably, enforcement should always entail the right to private legal action before an impartial and independent tribunal.

The *accountability principle* of the OECD Privacy Guidelines relies on the principle of enforcement/redress, but both principles are not the same. Accountability is more focused on assigning liability to the responsible entities/authorities for ensuring the protection of privacy and is more emphasized "on showing how responsibility is exercised and making this verifiable",[64] i.e. requiring data controllers to implement measures for upholding the data protection principles and to demonstrate that the measures taken are both appropriate and effective.[65]

[64] Article 29 Data Protection Working Party, WP 173, Opinion 3/2010 on the principle of accountability, Adopted on 13 July 2010, p. 7.

[65] *Ibid.*

Both enforcement and accountability require the identification of the responsible entities/authorities, which are primarily, at present, the relevant data controllers and/or processors. According to the OECD Privacy Guidelines, similar to Directive 95/46/EC, data controllers are the responsible entities or persons "competent to decide about the contents and use of personal data". However, identifying the responsible data controllers is not always easy, especially as a result of the increase in cross-border data flows and the complexity of information systems. Moreover, while the existence, nature and content of enforcement mechanisms can be assessed, "[t]he assessment of adequacy will be incomplete to the extent that it cannot assess actual practices and the realities of compliance".[66]

With regards to enforcement/redress and accountability, the following are some questions that should be addressed, where applicable:

1. What enforcement mechanisms are available?
2. If available, what are the specific legal sources that establish the enforcement mechanisms?
3. Are both judicial and non-judicial remedies available for data subjects?
4. Is the right to private legal action available?
5. Can data controllers be held criminally liable for serious privacy violations? Are they also subject to civil action and penalties?
6. Can the injured data subjects be rewarded monetary compensation for these violations? Are the criminal sanctions and monetary sanctions sufficiently rigorous to ensure compliance?
7. Is there a supervisory public authority responsible for overseeing compliance? What are the enforcement powers of this supervisory public authority and how independent or impartial is it?

(6) *Purpose Specification*

The *purpose specification* principle requires that the purposes for which personal data is lawfully collected must be transparent and specified beforehand (usually in writing), and its subsequent processing (collection, use, retention, modification, analysis, distribution, etc.) must be limited to the fulfillment of those specific purposes and not

[66] "Application of a methodology designed to assess the adequacy of the level of protection of individuals with regard to processing personal data: Test of the method on several categories of transfer", Final Report presented by the University of Edinburgh on behalf of: Charles D. Raab, Colin J. Bennett, Robert M. Gellman, and Nigel Waters, September 1998, European Commission Tender No. XV/97/18/D, p. ii, available at: http://ec.europa.eu/justice/policies/privacy/docs/studies/adequat_en.pdf

contrary to them. The purpose specification principle also holds that personal data should not be retained for longer than necessary to fulfill those purposes. Once its retention is no longer necessary to fulfill the specified purpose for which it was collected, data controllers must then delete or destroy the relevant personal data or, at minimum, unequivocally anonymize the personal data.[67] The principle is considered essential since "informed consent to the collection and processing of his/her personal data is dependent on the information about the purpose and use of those data" (Tzanou, 2010, p. 421). The purpose specification principle, for instance, is embodied in Article 6.1(b) of the EU's Data Protection Directive (Directive 95/46/EC).

With regards to purpose specification, the following are some questions that should be addressed, where applicable:

1. What are data subjects informed concerning the purpose of the data collection?
2. Are there any legally binding restrictions on the purposes for which personal data can be collected?
3. How is it determined that personal data is no longer needed to fulfill the specified purpose for which it was collected?

(7) *Use Limitation*

The *use limitation* principle requires that personal data should not be used in any way beyond the originally stated objectives for which it was collected, unless with the explicit consent of the concerned data subject or explicitly permitted by law. The use limitation principle helps to prevent "function creep". Function creep occurs when "personal data collected for one specific purpose and in order to fulfill one function, are used for completely different purposes, which are totally unrelated to the ones for which they were initially collected".[68]

With regards to use limitation, the following are some questions that should be addressed, where applicable:

1. When are the originally stated objectives deemed to have been achieved?
2. How can data subjects be sure that their personal data is not used beyond what they have been informed of and have originally consented to?

[67] see OECD Privacy Guidelines, Explanatory Memorandum, para. 54.

[68] Tzanou, Maria. *The EU as an Emerging Surveillance Society: The Function Creep Case Study and Challenges to Privacy and Data Protection* (4 Vienna Online Journal on International Constitutional Law, 2010), p. 421.

(8) *Proportionality*

The *principle of proportionality* is a general legal principle often used in both domestic criminal law, to represent the notion that the punishment for a criminal offense must be relative to its gravity, and in international law, to regulate a state's use of armed force during a conflict, whereby the harm brought upon civilians and civilian infrastructure must be relative to the intended lawful and specific military objectives sought after.

The legal principle of proportionality also effectively applies to privacy/data protection law. As widely recognized, the legal principle represents the notion that the processing (collection, use, retention, modification, analysis, distribution, etc.) of personal data and/or the infringement upon privacy, whether based on consent or not, should be necessary, reasonable, appropriate, relevant and not excessive in relation to the specific, legitimate purpose(s)/aim(s) for doing so (e.g. security gains), in accordance with the law in a free and democratic society.[69] The principle of proportionality is applicable, regardless of the purported legitimate purpose(s)/aim(s) sought after. In addition, as widely understood, the principle of proportionality also applies to the chosen means/measures (i.e. method, technology, etc.) used. If less intrusive or more reasonable means/measures are available to equally achieve the same legitimate aim(s), then those means should arguably be chosen instead. Accordingly, both the relevance of the purported legitimate aim(s) and the factual circumstances and consequences of the employed means must be considered (for further discussion, see, e.g., Taylor, 2002a).

Specifically, in terms of data protection, the principle of proportionality is also connected with the *data minimization principle* and the *collection limitation principle*, which collectively require that no more data should be collected than is required for the specified purpose(s)/aim(s) of its collection and that the personal data should only be obtained through lawful means.

[69] see, e.g., Charter of Fundamental Rights of the European Union, Article 52(1).

3.5 THE EUROPEAN APPROACH VS. THE AMERICAN APPROACH

Again, there is indeed consensus among Western free and democratic nations over the fundamental principles of privacy, but there are differences of opinion, particularly between policy makers/lawmakers in the EU and the US, over how to best implement the fundamental principles and what the machinery of enforcement and redress should entail.[70] These differences, some of which were previously highlighted by Bennett (1992) and Reidenberg (2000), are still valid.[71]

Among EU Member States, there is somewhat broad agreement that privacy principles and data protection rules must be codified in legally-binding legislation and backed by an independent, dedicated, central/national and governmental supervisory agency with the authority to investigate complaints, ensure compliance and impose sanctions for non-compliance. This agreement was manifested in the adoption of Directive 95/46/EC – a comprehensive, broad, multi-sectoral privacy legislation that regulates practically all data collection/processing activities, regardless of the technology concerned, of both private entities and public authorities (except for law enforcement agencies). The EU's regulatory approach is thus technology-independent. Accordingly, each EU Member State has passed domestic legislation transposing Directive 95/46/EC and has established a national data protection supervisory authority. As Reidenberg (2000) points out, although there are varying legal interpretations of Directive 95/46/EC within the EU, there is clearly a "common view that data protection is a basic human right that must be guaranteed by the state". The European legal approach has had a direct influence on the legal frameworks of other countries outside the EU, such as Australia, New Zealand, Japan, South Africa and Canada (Birnhack, 2008).[72] Nevertheless, while legally binding 'hard' laws are customary for protecting privacy in Europe, self-regulations (or non-legally binding 'soft' laws) are also occasionally relied upon.[73]

---

[70] The current negotiations between the US and EU over a future binding transatlantic agreement on the exchange of data for law enforcement purposes and the protection of privacy thereof may highlight these differences.

[71] For further discussion, see Bennett, Colin. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Cornell University Press, 1992).

[72] Birnhack, Michael D. *The EU Data Protection Directive: An Engine of a Global Regime* (Tel Aviv University Law Faculty Papers, Paper 95, 2008).

[73] see Bignami, Francesca. *The Non-Americanization of European Regulatory Styles: Data Privacy Regulation in France, Germany, Italy, and Britain* (Center for European Studies Working Paper Series #174, 2010), available at: http://www.ces.fas.harvard.edu/publications/docs/pdfs/CES_174.pdf

The US legal approach to protecting privacy is based instead on a unique mixture of separate statutory laws for various subject matters/technologies/domains, case law and self-regulations. In particular, the US approach is sectoral rather than all-inclusive or comprehensive, which is partly the cause for some of the deficiencies or gaps in the US legal framework, as explained in the subsequent chapters of the dissertation. The US regulatory approach is thus technology-dependent. Moreover, the US Congress often passes laws only after a serious problem or incident arises and not before. As Reidenberg (2000) similarly points out, under the US approach, the "law only intervenes on a narrowly targeted basis to solve specific issues where the marketplace is perceived to have failed". Still, the US has not successfully passed legislation similar to the EU's Directive 95/46/EC. The Privacy Act of 1974, for instance, is nowhere near as comprehensive and broad as Directive 95/46/EC and nor does it apply to private entities. While there are other specific privacy protection laws for different subject matters, domains or technologies, voluntarily adopted self-regulations/industry codes of conduct/corporate practices are instead primarily relied upon, at present, to safeguard privacy in the US (Reidenberg, 2000). Data controllers are free to formulate these regulations and are primarily responsible for ensuring their compliance.

However, although in the US there is no dedicated, governmental supervisory authority, equivalent to the national data protection supervisory authorities in EU Member States, to enforce compliance with privacy rules, the enforcement of corporate self-regulations/privacy policies are supervised by the FTC. The FTC has the authority to act against unfair and deceptive practices or broken promises. While the FTC is the closest body in the US to a national data protection supervisory authority, there is also in the US the Privacy & Civil Liberties Oversight Board.[74] There are also offices of privacy protection on the state-level, but the responsibilities of these bodies are merely advisory.

On the other hand, as Bignami empirically reveals, tort litigation for privacy violations in the EU still plays a relatively insignificant role compared to within the US. Instead, administrative redress plays a more significant role in the EU. However, as Bignami also reveals, the number of tort litigation cases for privacy violations in the EU has

[74] The Privacy and Civil Liberties Oversight Board (PCLOB) was established after the National Commission on Terrorist Attacks Upon the United States (known as the 9/11 Commission) recommended it. The PCLOB is an independent agency within the executive branch and is meant to provide oversight in the fight against terrorism. But, the PCLOB is still inactive.

steadily increased since the adoption and transposition of Directive 95/46/EC,[75] which provides for judicial remedy and the awarding of compensation for privacy violations.[76]

In accordance with the OECD Privacy Guidelines, however, there is essentially no single, correct way of enforcing or implementing the privacy principles, as long as they are indeed enforced or implemented in practice. In actual fact, the OECD Privacy Guidelines explicitly "permits Member countries to exercise their discretion with respect to the degree of stringency with which the [OECD Privacy] Guidelines are to be implemented, and with respect to the scope of the measures to be taken",[77] and does "not presuppose their uniform implementation by Member countries with respect to details".[78]

In spite of this, for the sake of this dissertation, the assessment of the adequacy of enforcement/redress mechanisms is, for the most part, based on the European approach.

3.6 REQUIRED LEGAL CHARACTERISTICS

In parallel with the application of the fundamental privacy principles, there are other legal characteristics that should arguably be considered when assessing the adequacy and soundness of a legal framework in terms of privacy protection. Based on these required legal characteristics, other legal deficiencies and dilemmas in the legal framework can also be determined.

In terms of ensuring the protection of privacy, the legal framework should also be:

- Legally binding, 'hard', actionable and enforceable;
- Consistent;[79]
- Precise, clear[80] and not ambiguous;[81]

---

[75] Prof. Francesca Bignami presented her empirical analysis at the third annual international conference *Computers, Privacy and Data Protection* (January 29-30 2010, Brussels), which I attended.
see Bignami, Francesca. *The Non-Americanization of European Regulatory Styles: Data Privacy Regulation in France, Germany, Italy, and Britain* (Center for European Studies Working Paper Series #174, 2010), available at: http://www.ces.fas.harvard.edu/publications/docs/pdfs/CES_174.pdf

[76] see Articles 22 and 23 of Directive 95/46/EC.

[77] OECD Privacy Guidelines, Memorandum, para. 45.

[78] *Ibid.*

[79] see Tamanaha, Brian Z. *On the Rule of Law: History, Politics, Theory* (Cambridge University, 2004).

[80] see, e.g., *Khan v. United Kingdom*, Application no. 35394/97, Judgment of 12 May 2000, §26.

[81] see Tamanaha, Brian Z. *On the Rule of Law: History, Politics, Theory* (Cambridge University, 2004).

- Free of vague concepts and/or definitions;
- Free of legal loopholes;
- Foreseeable (the law should be of such quality and precision that determining when it has been complied with or breached is apparent and predictable, and if breaches are permitted, then the justification for doing so must also be precise and clear):[82]
- Readily accessible;[83]
- Flexible, but also specific, where and when needed;
- Up to date with current PITs and anticipatory of their further advancement;
- Not primarily dependent on self-regulations, whether governmental or private;
- Not primarily dependent on case law;
- In compliance with relevant international norms and other legal instruments; and
- Not completely contrary to the recommendations of international organizations, such as the OECD, United Nations and Council of Europe, or perhaps the domestic laws of other countries widely considered democratic and free.[84]

If any legal framework or legal practice is contrary to or lacks any of these required legal characteristics, where applicable, then the law may be inadequate, to a certain extent or degree, depending on the extent and scope of the contradiction and deficiency.

3.7 BASIC PRE-MEASURES

In addition, based on both common practices and the privacy principles, other basic measures should arguably be carried out before any relevant law is enacted, policy adopted, policy instrument implemented or PIT deployed. These basic pre-measures may include:

- An assessment of the impact upon privacy;
- Identification and testing of possible alternative means for achieving the same end in a less intrusive manner; and
- Public engagement with relevant stakeholders, requesting public input/comments, and taking into account the concerns of the general public.

---

[82] see, e.g., *Kopp v. Switzerland*, Application No. 23224/94, Judgment of 25 March 1998.

[83] *Ibid.*

[84] Of course, what makes a country “democratic and free” is a whole other question, which requires its own set of criteria.

3.8 LEGAL CRITERIA SPECIFIC TO THE US

In the US, the law must be capable of upholding the integrity of the US Constitution, in particular the freedom from unreasonable search and seizure enshrined in the Fourth Amendment. Where applicable, the law must comply with the Privacy Act of 1974 and other relevant statutory laws, both federal and state.

3.9 LEGAL CRITERIA SPECIFIC TO THE UK

In the UK, the law must be capable of upholding the right to a private life, as enshrined in Article 8 of the European Convention on Human Rights (ECHR) and incorporated into domestic law through the Human Rights Act (1998). The law should comply with judgments of the European Court of Human Rights (ECtHR). All UK laws must comply with the principles enshrined in the Data Protection Directive and the Data Protection Act (1998), which incorporates the EU Directive into UK law. Moreover, UK lawmakers should equally take into consideration the recommendations and opinions of the Council of the EU, the European Commission, the Council of Europe, the Article 29 Working Party and the European Union Agency for Fundamental Rights.

3.10 APPLYING THE PRIVACY PRINCIPLES OF THE 20TH CENTURY TO THE TECHNOLOGICAL ADVANCEMENT OF THE 21ST CENTURY

As reaffirmed by OECD member states, during a 1998 conference in Ottawa, Canada and declared in a Ministerial Declaration on the Protection of Privacy on Global Networks:

> the technology-neutral principles of the 1980 OECD [Privacy] Guidelines continue to represent international consensus and guidance concerning the collection and handling of personal data in any medium, and provide a foundation for privacy protection on global networks.[85]

Indeed, however, the OECD Privacy Guidelines "were prepared in the context of the technology then known and envisaged," as the Hon Justice Michael Kirby, who chaired the expert group that produced the OECD Privacy Guidelines from 1978-80,

[85] Organisation for Economic Co-operation and Development, Ministerial Declaration on the Protection of Privacy on Global Networks, Ottawa, 7-9 October 1998, DSTI/ICCP/REG(98)10/FINAL.

pointed out.[86] While the velocity and scope of the advancement of PITs since 1980 has been remarkable, the fundamental privacy principles formulated by the OECD can potentially still meet the technological challenges of the 21st Century and still remain applicable "irrespective of the particular technology employed".[87] However, the endless advancement and deployment of PITs equally requires new and specific guidance on how to apply the privacy/data protection principles in practice,[88] and may require further legislative and non-legislative action to ensure their effective application.[89]

Moreover, perhaps contrary to the OECD's earlier view, some of the principles, particularly the *use limitation* and *purpose specification* principles (in addition to the *principle of proportionality*), are not only applicable to the processing of personal information/data, but also to the protection of privacy in general. For the most part, the privacy principles can also potentially be adapted to address privacy violations no matter where and in which manner they occur. The continued relevance of the fundamental privacy principles is demonstrated by the case studies.

PART II (Chapters 5, 6, 7) evaluates/assesses the adequacy of the legal frameworks in the US and UK, based on the criteria outlined in this chapter, in light of the privacy-intrusive capabilities of the following four particular PITs: body scanners; CCTV microphones and loudspeakers; and human-implantable microchips (RFID implants; GPS implants).

---

86 Kirby, Hon Justice Michael. *Privacy protection, a new beginning: OECD principles 20 years on* (Privacy Law and Policy Report, Volume 6, No. 3), pp. 25-29, at 27, available at: http://www.austlii.edu.au/au/journals/PLPR/1999/41.html

87 OECD Privacy Guidelines, Explanatory Memorandum, para. 37.

88 see COM(2007) 87 final, Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive.

89 see COM (2009) 262 final, Communication from the Commission to the European Parliament and the Council - An area of freedom, security and justice serving the citizen.

PART II

4 Privacy-Invading Technologies

4.1 CHAPTER INTRODUCTION

Privacy-Invading Technologies (PITs) are rapidly advancing and are increasingly being deployed worldwide at an unprecedented pace.

Section 4.2 defines what is meant by PITs. Section 4.3 overall outlines the increasing threat posed by the growing deployment of PITs. Section 4.4 explains the overall threat to bodily privacy posed by PITs. Section 4.5 explains the increasing decline of privacy out in public, as a result of surveillance technologies and other PITs. Section 4.6 provides an overview of several other technologies that may pose a significant threat to privacy.

4.2 A DEFINITION OF PITs

A definition of PITs requires flexibility, in order to be broad enough to cover all existing, emerging and prospective technologies. For the purposes of this dissertation, Privacy-Invading Technologies/Privacy-Intrusive Technologies (or PITs) are generally defined as and encompass:

> *Any form or type of technology, whether hardware or software, product or service, which poses a particular threat to privacy and/or is capable of being used to substantially violate an individual's right to privacy and/or data protection rights.*

To some extent, however, nearly all information and communication technologies (ICTs) could be regarded as PITs, including, for example, the Internet, digital services, mobile phones, cameras, credit cards, electronic voting machines and even photocopiers.[90] Moreover, all technologies that enhance and/or replace human senses, particularly sight and hearing, is a PIT. Certainly, some PITs are more privacy-intrusive than others.

Therefore, PITs include not just ICT, but especially other types of technologies, such as DNA analysis systems, neurotechnology, identification technologies, nanotechnologies, advanced imaging technologies and mass surveillance technologies. For further discussion, see section 4.6.

4.3 THE GROWING DEPLOYMENT AND THREAT OF PITs

In a post-9/11 world, amid the GWOT (now instead referred to by the White House under the Obama Administration as the "Overseas Contingency Operation"), PITs, particularly surveillance technologies used by law enforcement agencies, are rapidly being developed and deployed on a global scale. The increasing technological development and availability of PITs is likely driven by the increasing collective demand from governments, companies and individuals for their widespread use. Governments, businesses and private individuals alike are collectively spending hundreds of billions of dollars on (homeland/national) security and surveillance technologies. A "culture of fear", whereby society fearful of the event of terrorism and/or violent crime, has fuelled the 'security-industrial complex' (Furedi, 2006) and has likely sparked this new and profitable 'economy of fear'.

A partnership between the public and private has evolved further, as a result. This merger of the agency of governments and corporations into a symbiotic relationship based on mutual wants is being justified not just in the name of security, but also for convenience, efficiency, personalized service, commercial advantages and for preventing fraud. However, for instance, as Masters and Michael (2006) point out, "[w]hile the safety and security argument has obviously paved the way for some new technologies in response to the new environment of terrorism and identity fraud, there is now a concern that further advancements will begin to infringe on the freedoms that security paradigms were originally designed to protect" (Masters and Michael, 2006, p. 37).

As pointed out in the study, *An Appraisal of the Technologies of Political Control*, prepared by the Omega Research Foundation in 2000 for the European Parliament's STOA panel, the advancement of surveillance technologies, in conjunction with other crowd control technologies, are instruments of political and social control and powerful

---

90 Investigative journalism in the US has uncovered the potential for multi-purpose photocopiers to reveal sensitive personal information stored on their hard drives. see Werner, Anna. "Office copiers can present identity theft risk" (CBS, 5 February 2010), available at: http://cbs5.com/investigates/copier.identity.theft.2.1471886.html

means of monitoring and discouraging internal dissent. The study further argues that in the foreseeable future, technology will most likely play the most important role in curtailing civil liberties.[91] The STOA panel made that prediction more than a decade ago.

If privacy and individual liberties are as dangerously at stake as easy to infringe upon, then the rapid and continuous technological advancement and deployment of PITs has, and will increasingly continue, to seriously jeopardize civil and political liberties. The latest PITs, and their radical privacy-intrusive capabilities and enormous potential for abuse, are leading to unprecedented intrusions into both our private and public space, threatening not just the right to privacy, but other civil rights and our freedom and personal dignity overall.

4.4 PITs AND THE HUMAN BODY

The private sphere encompasses an individual's personal space, private property, place of residence, personal belongings, domestic affairs, physical body, etc. Accordingly, the power of government authorities/law enforcement agencies, in free and democratic countries, over the private sphere is significantly restricted, in comparison to their power over the public sphere. An individual's physical body (i.e. the human body), in particular, concerns the most intimate or personal aspect of the private sphere and its protection is clearly an indispensable element of privacy altogether.

It is commonly recognized that the privacy of the human body, or "corporeal privacy", pertains to the privacy of one's genitalia, brain, genetic data and integrity of one's physical self, including the prohibition of removing objects/materials/liquids from one's body or inserting objects/materials/liquids into one's body by force or without that person's consent (albeit certain exceptions may apply for only legitimate purposes).[92] In short, corporeal privacy prohibits the undue scrutiny of/intrusion upon one's physical body without his/her consent. Corporeal privacy also involves the right to make certain autonomous decisions concerning one's physical body, which would partly explain why sexual preferences, reproduction, abortion and vaccinations are all considered privacy issues. Accordingly, corporeal privacy also prohibits forced abortions, forced sterilizations and normally forced vaccinations.

---

[91] Crowd control technologies, An appraisal of technologies for political control, Final Report to the STOA (Omega Foundation, 2000), available at: http://www.europarl.europa.eu/stoa/publications/studies/19991401a_en.pdf

[92] For example, police can forcibly request a breath sample (or even a blood sample) from a driver involved in an automobile accident to determine the driver's blood alcohol content (BAC) level. Or, medical personnel may perform required emergency operations/procedures on an individual, without that person's consent, if, for instance, he/she is unconscious.

Above all, the intrusion upon an individual's private parts or genitals, by force or without that person's consent, can lead to the utmost affliction of personal indignity, dishonor or humiliation. "[B]asic concepts of human dignity dictate a course of the utmost caution before an intrusion into the most private parts of the human body is allowed".[93] For instance, as the 8th Circuit Court in the US declared, "a strip search, regardless how professionally and courteously conducted, is an embarrassing and humiliating experience".[94] The 9th Circuit Court has also held that "[t]he desire to shield one's unclothed figure from [the] view of strangers, and particularly strangers of the opposite sex, is impelled by elementary self-respect and personal dignity".[95]

In essence, the human body is a key target of PITs. As Haggerty and Ericson point out, "[a] great deal of surveillance is directed at the human body" (2000, p. 611). The human body has become "an assemblage comprised of myriad component parts and processes which are broken-down for purposes of observation", which will ultimately transform "the body into pure information, such that it can be rendered more mobile and comparable", for the purpose of "developing strategies of governance, commerce and control" (*Ibid*., p. 613). Similarly, as Lee A. Bygrave argues, recent technological developments have led to the mining of the human body for ever-greater amounts of information.[96]

From the advancement of visualization or imaging technology, such as body scanners, to DNA analysis, HIMs, biometric identification technology, and neurotechnology, the focus of PITs on the human body has never been greater. With the emergence of HIMs, the human body may also become both generators and transmitters of information themselves, changing not just the level of privacy we enjoy over our bodies, but also the way we perceive our bodies. Yet, the current legal framework pertaining to privacy/data protection was evidently designed, for the most part, to control personal data, as conventionally understood, and not necessarily to regulate the extensions of privacy infringement into other domains, such as the human body (Wood, 2006, p. 89).

Chapter 5 specifically focuses on the latest PIT capable of infringing upon the privacy of the human body and practically rendering clothes as an obsolete means of shielding our naked bodies or genitalia – *Body scanners*.

93 *Security and law enforcement employees, District Council 82, American Federation of State, County and Municipal Employees, AFL-CIO v. Hugh CAREY, as Governor of the State of New York, et al*., 737 F.2d 187 (2nd Circuit, 1984).

94 *Hunter v. Auger*, 672 F.2d 668, 674 (8th Circuit, 1982).

95 *York* v. Story, *324 F.2d* 450 (9th Circuit, 1963).

96 see Bygrave, Lee A. *The body as data? Reflections on the relationship of data privacy law with the human body* (The edited text of a speech given at an international conference organized by the Office of the Victorian Privacy Commissioner on the theme "The Body as Data", Federation Square, Melbourne, 8 September 2003).

4.5 PITs AND THE PUBLIC SPACE

The nature of the public sphere (or public space)97 has changed, as a result of the increasing development and deployment of technologies and infrastructures capable of mass surveillance. Indeed, during the beginning of the 21st Century, we have witnessed the rapid disappearance of any remaining expectation of privacy in public, particularly in major urban areas and especially in the US and UK.

In the Western world, the US and UK, in particular, are gradually moving towards a "surveillance society"[98] of a scale and capacity never seen before, where everyday life is monitored, physical movements are tracked, most incidents/events can potentially be monitored/recorded and practically every person can potentially be watched and listened to without their acknowledgement/consent (see, e.g., Lyon, 2001). The advancement of technologies capable of mass surveillance has enabled both governments and private entities to potentially keep a vigilant and omnipresent eye and ear on the masses out in public. As a result of the rapidly increasing advancement, deployment and use of CCTV cameras (combined with microphones, loudspeakers and face recognition software/systems),[99] UAVs, GPS technology and its applications, RFID technology and its applications, Geographic Information Systems (GIS), Google's Street View, Automatic License Plate Recognition (ALPR) systems, Intelligent Transport Systems (ITS),[100] mobile phones as a tracking tool, and location-based services/location-aware

---

97 The public sphere includes, for instance, public parks, squares, sidewalks, etc. Semi-public spaces (or pseudo-public spaces) include, for instance, sports stadiums and shopping malls.

98 David Lyon describes a "surveillance society" as "a situation in which disembodied surveillance has become societally pervasive". Lyon, David. *Surveillance Society: Monitoring Everyday Life* (Open University Press, 2001), p. 33.

99 Face recognition software is even being integrated within online applications, for example, within websites such as Facebook and Face.com. Google Goggles, which allows users to search online (via Google images) for objects they have taken photos of, could also just as easily incorporate face recognition software, allowing users to also search online (via Google images) for persons they have taken photos of.

100 As explained by the EDPS, Intelligent Transport Systems (ITS) refer to the deployment of ICT (geolocalization technologies, such as GPS and contact-less technologies, such as RFID) within different transport modes, which will facilitate the provision of a variety of public and/or commercial LBS, such as real-time traffic information, eFreight, and eCall, and in doing so collect and process vast amounts of data from public and private sources. The deployment of ITS will support the development of applications for 'tracking and tracing' of vehicles and goods. see European Data Protection Supervisor Opinion on the Communication from the Commission on an Action Plan for the Deployment of Intelligent Transport Systems in Europe and the accompanying Proposal for a Directive of the European Parliament and of the Council laying down the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other transport modes, 22 July 2009, available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-07-22_Intelligent_Transport_Systems_EN.pdf

applications (which collect and retain electronic records of people's movements within public space), residents of the US and UK may essentially be subject, in many ways often involuntarily and sometimes unknowingly, to constant surveillance.

As mass surveillance becomes a reality, people will increasingly no longer be able to freely perform daily and lawful activities out in public, without being watched, tracked or listened to by either public or private entities.[101] Due to the widespread deployment of sophisticated CCTV systems, especially in urban areas, it is already difficult to escape ever-vigilant and omnipresent observation or to enjoy simply wandering around without being paid any attention to. For Gavison (1980), anonymity is a crucial element of privacy and enables the freedom/ability to carry out activities in public without necessarily "being the subject of attention", whereas "the aspect of anonymity that relates to attention and privacy is that of being lost in a crowd" (1980, p. 434). However, due to the significant tracking capabilities of mobile phones/smartphones and the potential widespread deployment of the identification/tracking capabilities of RFID technology, advanced CCTV camera surveillance systems (face recognition, etc.) and biometric technology, anonymity will no longer be an established notion of the public space and "being lost in a crowd" (Gavison, 1980, p. 434) is now gradually becoming more and more unexpected.[102]

In reality, the public sphere (i.e. streets, sidewalks, etc.) obviously never had the same level of privacy as the private sphere (e.g. a place of residence). However, it is arguably fair to assume that people, only just over a decade ago, generally viewed public spaces, in theory, as areas/zones where they still remained relatively anonymous or could be relatively left alone and not paid any attention to (for further discussion, see Gavison, 1980). Indeed, the ongoing rapid deployment of mass public surveillance technologies has led to the current debate on the level of privacy out in public. Beforehand, it was not really a matter of serious discussion. Although we have always known that our actions could be seen or our words could be heard in public by other people relatively nearby, only up until recently, people expected not to be closely monitored and publicly scolded from afar, for example with public CCTV cameras and CCTV loudspeakers, and they did not expect their actions and movements to be recorded and stored indefinitely for potential further processing. In other words, as Taylor points out, it is fair to say that "we all carry out acts in public that we would consider to be of a 'private' nature, where subjectively, we might have exhibited an expectation of

---

[101] For further discussion, see Lyon, David. *Surveillance Society: Monitoring Everyday Life* (Open University Press, 2001).

[102] For further discussion, see Blitz, Marc Jonathan. Video *Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity* (Texas Law Review, Vol. 82, No. 6, 2004), pp. 1349-1481.

privacy" (2002a, p. 74). Taylor further adds, "[t]hough the expectation of privacy may be considerably reduced in a public setting, this does not automatically mean that all privacy is lost" (2002a, p. 75). Therefore, while we certainly may still expect to be seen and heard when out in public, to a limited extent, we should not accept to be unduly identified, tracked, monitored, recorded and disturbed, and systematically observed and scrutinized or even potentially humiliated in public.

The degree of surveillance out in public is only getting worse and could ultimately get out of hand. As Monmonier points out, "[o]ne need not be a science fiction fan to envision a future in which cameras as dense as streetlights feed images to central computers with face-recognition algorithms and biometrics software that match pedestrians to their stored profiles and track their movement through streets and parks" (2004, p. 115).

Enhanced public surveillance CCTV systems, however, are just one component of a public mass surveillance grid; "ubiquitous computing" (ubicomp)[103] and/or "ambient intelligence" (AmI)[104] are other components.[105] Ubicomp, which may also be known as pervasive computing,[106] is the widespread (or ubiquitous) embedding of tiny, networked processing/computing devices or microchips into the very fabric of urban infrastructure and everyday objects. In addition to tiny, networked microchips and wireless sensors, RFID technology is central to ubicomp/AmI. AmI "refers to electronic systems that are sensitive and responsive to the presence of people"[107] and the integration of these electronics into the surrounding environment, enabling for human interaction with the environment.[108] GPS technology could equally become ubiquitous and evolve beyond mobile devices to their 'embedded' form.[109]

---

[103] Mark Weiser first introduced the concept of "ubiquitous computing" during the 1990s. see Weiser, Mark. *The Computer for the Twentieth-First Century* (Scientific American, Vol. 265, No. 3, September 1991), pp. 94-104.

[104] see Aarts, Emile., and Boris de Ruyter. New research perspectives on Ambient Intelligence (Journal of Ambient Intelligence and Smart Environments I, 2009), pp. 5-14, at 5.

[105] As also highlighted by the SWAMI (Safeguards in a World of Ambient Intelligence) project, "ambient intelligence" may pose a serious threat to privacy.

[106] Pervasive computing is similar to ubiquitous computing, only that the former emphasizes interoperability and seamless interconnectivity. see Aarts, Emile., and Boris de Ruyter. *New research perspectives on Ambient Intelligence (Journal of Ambient Intelligence and Smart Environments I*, 2009), pp. 5-14, at 6.

[107] *Ibid., p. 5*

[108] *Ibid.*

[109] see Cave, J., et al. Trends in connectivity technologies and their socio-economic impacts, Final report of the study: Policy Options for the Ubiquitous Internet Society, (RAND Europe, July 2009), p. 30.

Surveillance, therefore, may also come from not just the obvious or usual suspects, but additionally from the gradual testing and deployment of tiny, networked wireless sensors, which can, for example, measure or respond to temperature changes, sound, chemicals and odors. The widespread deployment of these sensors will create what is now known as a "ubiquitous sensor network" (USN), whereby the various sensing capabilities will bring about 'intelligent environments' and a 'single information space'.

Cities adopting ubicomp/pervasive computing and/or AmI and extensively deploying wireless sensors and next generation wireless networks (e.g. Broadband Convergence Network (BcN) or Wireless Broadband (WiBro)), are currently known as "ubiquitous cities" or "U-cities", which is essentially just another name for what is more commonly known as "smart cities". In U-cities, ICT is effectively ubiquitous and more than ever prevalent in people's daily lives, and extensively integrated into urban space and public infrastructure, linking the physical world with the virtual world, and integrating commercial, public, financial and medical data systems into a 'single information space'.

On the other hand, South Korea, rather than the UK and the US, is pioneering the development of U-cities and is currently engaged in numerous multi-billion dollar projects to develop the cities of tomorrow. Hwaseong-Dongtan, Busan and the New Songdo City are the most significant examples. The extensive deployment of ICT-related technological solutions, such as smart meters, telemedicine, e-Government and intelligent transport systems, together with sophisticated public surveillance systems, can potentially improve energy efficiency, improve healthcare delivery, enhance the provision of public services, reduce traffic congestion and increase public safety respectively. However, the corresponding privacy issues are also a serious concern.

Nevertheless, with the deployment and use of public transportation smart cards, electronic identification (eID), intelligent transportation systems, GPS-enabled smartphones, e-Health technologies, RFID technology and enhanced, networked CCTV surveillance cameras, for example, we are already witnessing the beginnings of a ubiquitous information society in cities across the US and Europe, albeit not on the full scale and scope of the emerging U-cities in South Korea.

In addition, sensors and other surveillance technologies are not only being deployed in public spaces, but also increasingly in homes, as part of the ICT-enabled solutions for independent living for the elderly, known as Ambient Assisted Living. These sensors and technologies can monitor a variety of activities in one's home. The assisted living solutions range from video monitoring systems to motion sensors that detect falls and other sensors embedded within domestic appliances and the extensive deployment/use of RFID tags/microchips. Collectively, the deployment of these sensors and technologies may, therefore, also change the nature of private homes (i.e. the private sphere).

As ICT and other technologies become widely deployed and embedded within urban/public infrastructure and everyday objects, these technologies will also likely become ‘invisible’, so to speak, since people might no longer be able to see these technologies and, even if they can see them, might no longer really take notice of their ubiquitous presence.[110] Therefore, mass surveillance technologies, for instance, could equally become not just ubiquitous, but *banal* as well. Accordingly, the term “banal surveillance” may better describe this growing trend.[111] For example, people already do not always notice the ubiquitous deployment of CCTV cameras and yet they are clearly visible.[112]

Moreover, in radically changing the long-established nature of public spaces, technology capable of mass surveillance enters into a realm beyond privacy. The freedom of assembly, freedom of speech, freedom of movement and the right to be left alone are now all at risk. These freedoms are the cornerstone of a democratic and free society, and public spaces serve as the place to carry out strikes or demonstrations, to exercise the freedom of movement and freedom of speech, and to engage in legitimate political activism and public discourse. Therefore, as technologies capable of mass surveillance are also used as a means of social and political control, they pose the serious risk of also ‘chilling’ the free exercise of these fundamental freedoms, in addition to threatening the right to privacy.[113]

Some authors, for instance David Brin, welcome the changing nature of the public space and the overall erosion of privacy, due to the development and deployment of advanced technologies capable of widespread surveillance, and envisage the emergence of a “transparent society” somehow remarkably endowing society with the benefits of openness and accountability by practically allowing everyone to know and observe everything

---

110 In the words of Godfrey Reggio (the Director of the acclaimed film Koyaanisqatsi), “Technology has become as ubiquitous as the air we breathe, so we’re no longer conscious of its presence”. Welsh, James M., Gene D. Phillips, and Rodney Hill. *The Francis Ford Coppola Encyclopedia* (Scarecrow Press, 2010), p. 157.

111 I base the term “banal surveillance” on the term “banal nationalism”, coined by Michael Billig to describe the routine or unnoticed performance of nationalism in everyday life. see Billig, Michael. *Banal Nationalism* (Sage Publications, 1995). It is also important to note here, however, that today’s terminology used to describe tomorrow’s world and potential future scenarios could become outdated or inaccurate, since something quite different could easily manifest instead.

112 This may be similar to the ubiquitous and unnoticed deployment of national flags, which characterizes “banal nationalism”.

113 see *Crowd control technologies, An appraisal of technologies for political control, Final Report to the STOA* (Omega Foundation, 2000), available at: http://www.europarl.europa.eu/stoa/publications/studies/19991401a_en.pdf

and everyone else (Brin, 1999). While this was somewhat a novel idea, it is incomplete and, as Schneier significantly points out, “it ignores the crucial dissimilarity of power”.[114]

On the contrary, if left unchecked, especially without adequate safeguards in place, and with the (technological/scientific, economic and political) elite branch or power structure of society controlling the advancement and deployment of the most privacy-intrusive technologies, what could more likely emerge instead is the rise of a high-tech, dystopian, surveillance society or a so-called “technetronic society”. In *Between Two Ages: America’s Role in the Technetronic Era*, Zbigniew Brzezinski, a highly-respected actor in world affairs and the former US National Security Advisor (1977-1981), compellingly described this “technetronic society” decades ago:

> Such a society would be dominated by an elite whose claim to political power would rest on allegedly superior scientific know-how. Unhindered by the restraints of traditional liberal values, this elite would not hesitate to achieve its political ends by the latest modern techniques for influencing public behavior and keeping society under close surveillance and control (1970, pp. 252-53).

The deployment and use of technologies capable of mass surveillance might improve, for example, public security/safety, but without sufficient legal safeguards in place, it would do so by undesirably undermining the freedoms/liberties citizens seek to exercise and the relative sanctuary they seek to enjoy out in public spaces.

Chapter 6 focuses on the latest developments regarding public space CCTV cameras – the integration of *CCTV microphones* and *CCTV loudspeakers*. Chapter 7 addresses both the corporeal privacy and public surveillance implications of *Human-implantable microchips* and the corresponding RFID and GPS infrastructure, essentially outlining how HIMs alter/impact both the nature of the human body (private sphere) and the public sphere. HIMs, therefore, serve as a case study for both *PITs and the human body* and *PITs and the public space*.

[114] Schneier, Bruce. “The Myth of the ‘Transparent Society’” (Wired, 3 June 2008), available at: http://www.wired.com/politics/security/commentary/securitymatters/2008/03/securitymatters_0306

4.6 EXAMPLES OF PITs THAT MAY POSE SERIOUS THREATS TO PRIVACY AND LIBERTY

In addition to the four PITs specifically addressed in this dissertation (i.e. the case studies), there are many other PITs, either still in the R&D or innovation stages or have already been deployed and are in use, which present equally serious challenges, if not greater, to privacy and liberty. These other PITs include: open source information[115] data mining intelligent software[116] (part of open source intelligence (OSINT)[117] technologies); cookies; Fusion Centers; DNA analysis; electronic voting machines; automatic license plate recognition; intelligent transportation systems; unmanned aerial vehicles; ultra-thin, high-resolution cameras; Google's digital services (e.g. Google Voice, Google Street View, etc.); LEXID; Facebook (and other online social networking services); cloud computing services; automobile black boxes; Deep Packet Inspection software or behavioral advertising technology (e.g. Phorm); laptop/PC web-cams; nanoelectronics; software agents/artificial intelligence; Einstein 2;[118] and neurotechnologies. This list is certainly far from complete and does not even begin to cover the numerous other completed or ongoing publicly and/or privately funded projects that we know of (or do not know of) that are developing PITs.

---

[115] Open source information, as opposed to closed source or classified information, includes anything publicly available, whether online or offline, such as blogs, tweets, information posted on social networking sites, videos, web chats or any other user-generated content, online news, websites, public data, geospatial data, books, academic papers, newspapers, magazines and even book/movie reviews.

[116] The software and system being developed by Project INDECT or the software used by Visible Technologies can mine through infinite amounts of open source information, categorize this information and raise 'alarms'.

[117] Open Source Intelligence (OSINT) is the use of open source information for intelligence gathering and analysis. OSINT is increasingly being used by intelligence and law enforcement agencies around the world. OSINT is complementary to Human Intelligence (HUMINT), Signals Intelligence (SIGINT), Imagery Intelligence (IMINT) and Communication Intelligence (COMINT). We are seeing over and over that murderers and other criminals, and even lone terrorists, either brag about their crimes afterwards or give clues or clear warnings beforehand online. This is where OSINT comes in. If intelligence agencies or law enforcement agencies were able to monitor, sort and analyze all communications online, this could be used to apprehend the suspects or perhaps prevent the planned crime or act of terror. OSINT could also provide some early warnings of a looming crisis.

[118] Einstein 2 is a cyber intrusion detection system, developed by the United States Computer Emergency Readiness Team (US-CERT), meant to detect unauthorized traffic on governmental networks. Einstein 3 will go a step further and is meant not just to detect unauthorized traffic, but defend against it and attack the threat. However, in doing so, Einstein 3 is expected to collect and analyze the content of all communications, in addition to monitoring malicious software attack patterns, in the name of cyber-security. see Radack, Jesselyn. "NSA's cyber overkill" (Los Angeles Times, 14 July 2009), available at: http://articles.latimes.com/2009/jul/14/opinion/oe-radack14

The following is a brief explanation of the radical capabilities and new threats to privacy and liberty posed by the following five PITs: Neurotechnology; Unmanned aerial vehicles; LEXID®; DNA analysis; and Automatic License Plate Recognition.

4.6.1 Neurotechnology

Neurotechnologies are essentially technologies capable of determining and even perhaps intervening in the neural functioning of a human mind.[119] A number of neurotechnological applications are already available for general public use.

An example of the recent advancement in neurotechnology includes hypersonic sound (HSS). Developed by the American Technology Corporation, HSS provides the ability to direct sound to a specific area or target, similar to light, using ultrasonic sound energy. Thus, HSS can be potentially used to infiltrate an individual's brain and direct verbal communication to a particular person exclusively.

Other applications or examples of neurotechnology include Emotiv's commercially available brain-computer interface (BCI) technology that can read and interpret human thoughts, emotions and intentions to a certain degree. The information, for instance, can enable a computer game to respond to a player's emotions or enable an avatar (game character) mimic the expressions of the player.

Neuroscientists have even developed a way of turning thoughts into 'tweets' on Twitter, and the ability to use thoughts to move and control robotic arms or a wheelchair. Moreover, neuroscientists are working to develop new technologies to identify particular brain patterns, determined through brain scans, pertaining to certain behaviors, such as violence and lying. Neuroscientists have also successfully reconstructed patterns of brain activity into images to determine what the test subjects had seen.[120]

There are certainly societal benefits of neurotechnology, especially for the disabled, who either cannot move or are missing limbs or are bound to a wheelchair. As a result, there are significant R&D projects, in the US, EU and Japan, that are working towards neurotechnological solutions for handicapped persons. Neurotechnology also offers benefits for the mentally ill. However, it is questionable that these innovative R&D activities involving neurotechnolgy are taking into consideration the potentially

---

[119] For further information, see "Clive Thompson on Why the Next Civil Rights Battle Will Be Over the Mind" (Wired, 24 March, 2008), available at: http://www.wired.com/techbiz/people/magazine/16-04/st_thompson

[120] see Naselaris, Thomas., et al. *Bayesian Reconstruction of Natural Images from Human Brain Activit*y (Neuron, Volume 63, Issue 6, 902-915, 24 September 2009).

serious ethical issues and privacy threats at this early stage.[121] As the applications of neurotechnology steadily advance and the scope of use increases, grave privacy and security concerns will certainly increase accordingly, if privacy is not adequately considered from the very beginning.

Neurotechnologies clearly challenge a realm/domain of privacy never seriously considered before to be vulnerable to technology – the brain or mind, and essentially spark a new debate on mental privacy or privacy of the brain/mind[122] and the meaning of 'cognitive liberty' (or freedom of thought).[123]

4.6.2 Unmanned Aerial Vehicles

Unmanned Aerial Vehicles (UAVs) (also known as "drones") are aerial vehicles piloted by either artificial intelligence or by remote control, and are often used for surveillance/reconnaissance missions or air assaults. UAVs include, for example, the "Shadow", "Raven", "Zephyr" and "Predator". Other UAVs or drones include micro aerial vehicles (MAV), vertical take-off and landing (VTOL) vehicles or larger airships, such as blimps, and robotic helicopters, such as the A-160T Hummingbird.

The most advanced imaging systems/cameras are often attached to large or medium-sized UAVs, providing the ability to conduct continuous, wide-area visual surveillance from the air. The images or video feed are then transmitted in real-time to computers on the ground. Advanced imaging systems, developed under the auspices of the Defense Advanced Research Projects Agency (DARPA), include the Autonomous Real-time Ground Ubiquitous Surveillance - Imaging System (ARGUS-IS)[124] and Panoptes, an ultra-thin, lens-free, ultra high-resolution camera.

The increasing development, deployment and use of UAVs and advanced imaging systems have resulted in the need to monitor and analyze large amounts of video data.

---

[121] For example, the neuroscientists that I spoke with at the ICT Event 2010, who were demonstrating BCI technology applications, which they had developed, never considered any of the potential privacy or ethical issues associated with the technology.

[122] "Clive Thompson on Why the Next Civil Rights Battle Will Be Over the Mind" (Wired, 24 March, 2008), available at: http://www.wired.com/techbiz/people/magazine/16-04/st_thompson

[123] The non-profit law institute Cognitive Liberty and Ethics defines "cognitive liberty" as the "right of each individual to think independently and autonomously, to use the full spectrum of his or her mind, and to engage in multiple modes of thought". For further information, see http://www.cognitiveliberty.org/faqs/faq_general.htm

[124] ARGUS-IS is the integration of a 1.8 Gigapixels video sensor, an airborne processing subsystem and a ground processing subsystem.

In a broad agency announcement for contractors, DARPA described the "ever increasing need to monitor live video feeds and search large volumes of archived video data for activities of interest due to the rapid growth in development and fielding of motion video systems".[125] As DARPA explains, the capability of UAVs in recording huge swathes of video footage, which involves so many activities or objects to be watched for hints of "suspicious behavior" and their growing field of view (up to 25 km^2 in the near future), is making it evermore harder to effectively monitor and scrutinize/interpret all potential activities. An automated system, DARPA further explains, is therefore required to have the capability of simultaneously analyzing and detecting specific actions, events and activities in real-time and indexing and searching archived video, as opposed to the use of labor intensive human analysis of portions of real-time video and the manual review of archived video using normal fast forward and reverse controls.[126] This automated system is termed the Video and Image Retrieval and Analysis Tool (VIRAT) and DARPA is contracting software companies and universities to develop it. The resolution capability of the video system ranges from 10-30 cm, which DARPA has assured is not enough to permit human identification.[127] However, there are several multi-gigapixel cameras in development, such as Panoptes, which are more than capable of being used to identify individuals on the ground. VIRAT will be capable of looking for activities, such as loitering, running, smoking, hand shaking, kissing, fires, crowds, convoys and vehicles movements.[128] The focus of VIRAT is aerial video, but of course VIRAT can also be used for on ground-based video.[129]

In addition to foreign intelligence operations and military reconnaissance, UAVs can be used by law enforcement agencies for domestic routine aerial surveillance. The variety of potential public security/safety gains of the use of UAVs include their use in the surveillance of suspected criminals, search and rescue missions, border surveillance, neighborhood patrols, chemical and biological weapon detection, monitoring forest fires, floods and storms, and enforcing traffic laws. While UAVs are not yet commonplace, there is an increasing interest in their use. In a paper titled "Applications

125 Broad Agency Announcement, Video and Image Retrieval and Analysis Tool (VIRAT), DARPA INFORMATION PROCESSING TECHNIQUES OFFICE (IPTO), BAA 08-20, 03 March 2008, available at: https://www.fbo.gov/download/32f/32f2382440cfb57d2695171885acab57/virat_baa_08_20_final_3_3_08.pdf

126 *Ibid.*

127 *Ibid.*

128 *Ibid.*

129 *Ibid.*

for mini VTOL UAV for law enforcement", Douglas Murphy from the Space and Naval Warfare Systems Center in San Diego and James Cycon from Sikorsky Aircraft Corporation, reveal the support of the US Department of Defense in using UAVs for routine law enforcement and domestic surveillance and control.[130] In the UK, police are equally keen on using UAVs for domestic routine surveillance.[131] UAVs could also be used for crowd or riot control, with the attachment of the latest non-lethal weapons.

In the US, the FAA is (or at least was) the main barrier to the widespread deployment of UAVs for mass domestic aerial surveillance and routine law enforcement operations. The FAA has opposed the widespread deployment and use of UAVs in the US, based on air traffic/aviation safety concerns. At present, the FAA only authorizes the domestic use of UAVs on a case-by-case basis and has issued hundreds of certificates to federal, state and local law enforcement agencies.[132] But, as a result of the FAA Modernization and Reform Act of 2012, which requires the FAA to develop and implement operational and certification requirements for the deployment of UAVs as part of the national airspace system by the end of 2015, the routine and widespread deployment and use of UAVs is set to become a reality in the very near future.[133]

In addition to potential aviation safety concerns, there are also justified privacy concerns. Since case law in the US, for instance, permits law enforcement agencies to view or record what is in plain sight or open to the public eye,[134] it is likely that the general use of UAVs does not require reasonable suspicion or probable cause. Already, the use of manned police aircraft is legally permitted and considered reasonable for routine law enforcement activities or to gather evidence without a warrant.[135] But, there are still potential legal questions when, for instance, the surveillance is carried out to observe private residential backyards or to peek into high-rise apartment windows without a warrant. Nevertheless, the deployment/use of UAVs poses a greater threat to

---

[130] see Murphy, Douglas., and James Cycon. "Applications for mini VTOL UAV for law enforcement", available at: http://www.spawar.navy.mil/robots/pubs/spie3577.pdf

[131] see Lewis, Paul. "CCTV in the sky: police plan to use military-style spy drones" (The Guardian, 23 January 2010), available at: http://www.guardian.co.uk/uk/2010/jan/23/cctv-sky-police-plan-drones

[132] see Waterman, Shaun. "Drones over U.S. get OK by Congress" (The Washington Times, 7 February 2012), available at: http://www.washingtontimes.com/news/2012/feb/7/coming-to-a-sky-near-you/?page=1

[133] see *Ibid*.

[134] The US Supreme Court, for instance, held that there is no reasonable expectation of privacy in open fields. see, e.g., *Oliver v. United States*, 466 U.S. 170 (1984).

[135] The US Supreme Court in *Florida v. Riley*, 488 U.S. 445 (1989), for instance, ruled that law enforcement officers do not require a warrant to observe an individual's backyard from a helicopter hundreds of feet in the air.

privacy. For instance, manned police aircraft are not meant nor designed specifically for conducting mass aerial surveillance and nor do they have the most advanced imaging systems built-in. Moreover, UAVs could easily far outnumber ordinary manned police aircraft and they can fly for prolonged periods of time. Since UAVs can be much smaller and quieter, they can hover in areas where much larger manned aircraft cannot and their presence could also potentially go unnoticed. As potential vehicles for crowd control technologies and non-lethal weapons, UAVs could also have serious implications for other civil liberties.

4.6.3 LEXID®

The LEXID® (Lobster-Eye X-ray Imaging Device), being developed by Physical Optic Corporation and funded by the DHS, is an X-ray imaging hand-held device that provides the ability to view objects or persons behind walls or hidden in containers or vehicles.

The visualization or imaging technology of the LEXID® is modeled after the eyes of lobsters. Lobsters see by reflection, not refraction, made possible by thousands of squares located in their eyes. Composed entirely of straight walls and right angles, as opposed to the curved cones of a human's eye, a lobster's eye reflects light beams that enter at consistent angles. The consistency of these angles of reflection focuses all of the light beams to the same focal point, which enables lobsters to see in extremely dim light.[136]

The LEXID® consists of a low-powered X-ray generator and an optics system. Instead of detecting X-rays that pass through an object, the LEXID® detects X-rays that are scattered back to the device. The optics system, made up of thousands of polished metallic squares, acquires and focuses these backscattered rays by collecting all of the reflected rays into one focal point, instead of analyzing divergent rays at different points in the system. Software synchronizes the images acquired, then processes and displays them on a screen. The device, according to Physical Optics Corporation, can see through walls made of concrete or wood and even through steel up to 3 inches (75 mm) thick. Although the images are not perfectly clear, future systems are planned to have improved resolution.[137]

While the LEXID® offers potential security gains, people's homes and cars, for instance, are now more than ever vulnerable to unreasonable and warrantless searches conducted by law enforcement agents using this technology. If the use of LEXID® in-

---

[136] Physical Optics Corporation, available at: http://www.poc.com/emerging_products/lexid/default.asp

[137] *Ibid*.

deed becomes widespread and is left unchecked in the US and EU, the Fourth Amendment of the US Constitution or Article 8 of the ECHR / Article 7 of the Charter of Fundamental Rights of the European Union respectively will be rendered practically futile.

4.6.4 DNA analysis

Deoxyribonucleic Acid (DNA), now widely understood as the "genetic information molecule" of all living organisms, can be found in any human cell or bodily material, e.g. saliva, blood and strands of hair. Anything derived from a person's body can serve as a 'DNA sample'. A 'DNA profile' is generated from a DNA sample and is stored on a DNA database. The unique DNA characteristics are visualized as a numeric code.

While DNA profiles alone pose a far less threat to privacy than DNA samples, since the profiles are basically "just a bunch of numbers",[138] DNA profiles can still potentially reveal information on specific hereditary characteristics, depending on the chromosome zones used.[139] Moreover, in a process known as "familial DNA searching", DNA profiles can also be used to identify relatives, whereby a partial genetic match between two or more DNA profiles signifies that the individuals concerned are genetically related to one another.[140]

The analysis of a DNA sample, on the other hand, can reveal vast amounts of sensitive personal information, including details regarding physical characteristics, health and even certain behavioral traits. In the words of Sir Alec Jeffreys,[141] "[i]f you have a DNA profile it is just a bunch of numbers on the computer and it really does not matter, but if you have the original DNA sample then you have the potential to extract absolutely every scrap of genetic information of that individual".[142] The science and technology behind DNA analysis is advancing rapidly. Studies have now shown that "nearly all behaviors that have been studied show moderate to high inheritability - usu-

---

138 Sir Alec Jeffreys, House of Commons, Science and Technology Committee, Forensic Science on Trial, Seventh Report of Session 2004-05, para. 70.

139 see Council Resolution of 25 June 2001 on the exchange of DNA analysis results (2001/C 187/01).

140 For further discussion/explanation on the potentially significant privacy implications of "familial DNA searching", see Epstein, Jules. *"Genetic Surveillance" - The Bogeyman Response to Familial DNA Investigations* (Journal of Law, Technology and Policy, Vol. 2009, No. 1), pp. 141-173, available at: www.jltp.uiuc.edu/archives/Epstein.pdf

141 The British geneticist, Sir Alec Jeffreys, developed the standard DNA profiling techniques used today.

142 House of Commons, Science and Technology Committee, Forensic Science on Trial, Seventh Report of Session 2004-05, para. 70.

ally to a somewhat greater degree than do many common physical diseases" (McGuffin et al., 2001). Evidently, genes have an influence on behavior (Hood and Rowen, 1997). The MAOA gene is linked to violent behavior,[143] the D4-7 gene variant is known as the "risk-taking gene", the "stathmin" gene is responsible for fear and anxiety, and the CHRM2 gene is associated with intelligence (Dick et al., 2007). As research has shown, the information contained within a DNA sample could also potentially be used to construct a computer image of the source's face.[144]

People constantly leave behind DNA samples unintentionally and unavoidably. Since DNA samples are so easily left behind, a physical intrusion/abstraction is not necessary to obtain a DNA sample, and DNA samples can easily be obtained covertly. There are practically infinite possibilities on how a DNA sample could be covertly obtained. And, similar to trash discarded on public property, the collection of discarded DNA samples is, for obvious reasons, not illegal.[145] Even so, "[n]o surveillance technology is more threatening to privacy than that designed to unlock the information contained in human genes".[146] DNA is essentially everywhere and, as a result, could potentially or theoretically lead to what is known as "genetic surveillance"[147] or "bioveillance" (i.e. the omnipresent identification and tracking of individuals via the use of DNA), and even the business of "genetic paparazzi",[148] whereby the 'paparazzi' go around in search of DNA samples of popular figures, such as movie stars, in order to publicly reveal potentially hidden sensitive personal information about them for monetary rewards.[149]

The vast (sensitive) personal information contained within one's DNA still requires, however, sophisticated scientific expertise and advanced technology to be discovered.

143 see Russell, Jacob. "Genetic risk for violent behavior?" (UPI Correspondent, 27 November 2006), available at: http://www.upi.com/NewsTrack/Health/2006/11/27/genetic_risk_for_violent_behavior/9889/

144 see Goldman, Russell. "Crime Scene DNA Could Create Image of Suspect's Face" (ABC News, 18 February 2009), available at: http://abcnews.go.com/Technology/AheadoftheCurve/story?id=6897788&page=1

145 For example, the US Supreme Court, in California v. Greenwood, 486 U.S. 35 (1988), ruled that the warrantless search and seizure of trash discarded for collection is permissible.

146 Canadian Privacy Commissioner's report on Genetic Testing and Privacy (1992), p. 2.

147 For further discussion/explanation on the potentially significant privacy implications of "familial DNA searching", see Epstein, Jules. *"Genetic Surveillance" - The Bogeyman Response to Familial DNA Investigations* (Journal of Law, Technology and Policy, Vol. 2009, No. 1), pp. 141-173, available at: www.jltp.uiuc.edu/archives/Epstein.pdf

148 see Frumkin, Dan., et al. *Authentication of Forensic DNA samples* (Forensic Science International: Genetics, 2009).

149 *Ibid.*

Therefore, due to the high costs of DNA analysis, at present, "genetic surveillance" is not yet feasible. However, this could all change, as DNA analysis becomes more and more widespread, routine, cheaper and easier to perform.

Indeed, the cost of DNA sequencing/analysis has rapidly dropped in the last four years, at a much quicker rate of decline than computers, according to George M. Church, a pioneer in DNA sequencing technology and Professor of Genetics at Harvard University,[150] which has potentially given rise to a 'Moore's Law for DNA analysis'.[151] Already, at the cost of several thousand dollars, DNA tests can be conducted to determine if a person is prone to certain diseases. Web-based services, such as 23andMe, provide genetic home testing, which allows an individual to mail DNA samples for DNA analysis, normally to determine paternity. However, the most worrisome is relatively cheap and complete genetic sequencing.[152] Complete Genomics announced that the company will begin to charge $5,000 for the genetic sequencing of a human chromosome. The next step is $1,000 per genome, which is expected by 2012, and even newer techniques could drive the price down to $100 per genome.[153]

With regards to DNA analysis/sequencing, privacy is especially threatened by the risks of DNA samples being analyzed and used for additional unspecified purposes, without explicit consent or knowledge of the person concerned or beyond the original specified purposes the samples were collected with consent. As widely recognized, the risks of abuse are immense, due to the many ways in which the sensitive personal information contained within DNA samples can be wrongfully exploited. For instance, insurance companies may be interested in DNA analysis to predict a person's potential future health status or even potential driving skills,[154] when calculating premiums for insurance applicants. The results of the DNA analysis could provide the basis for a higher insurance premium. Employers could equally be interested in DNA analysis to also predict the potential future health status of job applicants or current employees and to determine the personality traits and intelligence of candidates. Accordingly, em-

---

150 see Pollack, Andrew. "Dawn of Low-Price Mapping Could Broaden DNA Uses" (New York Times, 6 October 2008), available at: http://www.nytimes.com/2008/10/06/business/06gene.html?hp

151 see Humphries, Courtney. "Over the Horizon: A Moore's Law for Genetics" (Technology Review, Published by MIT, March/April 2010), available at: http://www.technologyreview.com/biomedicine/24590

152 see *supra* note 148.

153 see *supra* note 149.

154 According to a recent study conducted by neuroscientists at the University of California in Irvine, a particular gene variant may be responsible for bad driving.
see http://uci.edu/features/feature_bdnfdriving_091028.php

ployers could use DNA analysis results to deny someone a job or promotion and could easily collect samples from employees without their knowledge or consent. Showing up at a job interview alone, for example, could supply the prospective employer with a DNA sample.

In the US, therefore, the Genetic Information Nondiscrimination Act of 2008 (GINA) was finally enacted and, as a result, employers are prohibited from taking employment-related decisions based on genetic information. GINA also prohibits health insurance companies from denying a person health insurance coverage or raising premiums based solely on genetic information. Nevertheless, what GINA explicitly covers is just the tip of the iceberg, when it comes to the foreseen and unforeseen possibilities, as outlined above, of using the potentially limitless sensitive personal information contained within DNA.

But, the covert nature of DNA sampling could mean one day that we could all be subject to DNA analysis without our knowledge or consent. Therefore, we could still gradually lose control of knowing when DNA analysis is conducted on us and how the results may somehow be used.[155] Accordingly, GINA, and similar legislation, will become increasingly difficult to enforce.

With the decreasing cost and increasing sophistication of DNA analysis and the potential for a DNA profile to be stored for every individual, DNA could one day be used for omnipresent identification and tracking or "genetic surveillance".[156] It could begin with not just police, but also with private companies, such as banks, demanding DNA samples to verify identity by using on-the-spot DNA sequencing. It is not as paranoid or farfetched as one might think. Already, according to responses to a review of the Police and Criminal Evidence Act (PACE), police in the UK have publicly proposed their desire to lower the threshold for which they can collect DNA samples to include non-recordable or non-imprisonable offences, such as littering and speeding, and the power to collect DNA samples simply to verify identity.[157] The storage of tens of millions of DNA samples and profiles, by governments and/or private entities, and both the

---

[155] For further discussion, see Article 29 Working Party, Working Document on Genetic Data, adopted March 2004 (WP 91), p. 12.

[156] see Epstein, Jules. *"Genetic Surveillance" - The Bogeyman Response to Familial DNA Investigations* (Journal of Law, Technology and Policy, Vol. 2009, No. 1), pp. 141-173, available at: www.jltp.uiuc.edu/archives/Epstein.pdf

[157] see Modernising Police Powers: Review of the Police and Criminal Evidence Act (PACE) 1984, Home Office, Consultation Paper, March 2007, para. 3.33; Ford, Richard. "Police want DNA from speeding drivers and litterbugs on database" (The Times, 2 August 2007), available at: http://www.timesonline.co.uk/tol/news/uk/crime/article2183105.ece; Travis, Alan. "Police may be given power to take DNA samples in the street" (The Guardian, 2 August 2007), available at: http://www.guardian.co.uk/politics/2007/aug/02/ukcrime.humanrights

decreasing cost and diminishing difficulty of DNA analysis, may inevitably lead to a society worried about unavoidably leaving behind vast amounts of (sensitive) personal information (i.e. DNA samples) wherever they go or whatever they do.

Her Majesty's Inspectorate of Constabulary (HMIC) has described DNA analysis as "by far the most significant breakthrough in crime detection since the inception of fingerprint identification".[158] Indeed, DNA profiles, generated from DNA samples obtained from crime scenes, have led to the identification of suspects responsible for murders and rapes, and significantly improved the chances of a crime being solved. For example, in the UK, at one point, with DNA profiling, the rate of detection increased to 43% from the average detection rate of 24%.[159] However, the faith in DNA as the "golden standard" of identification is now being called into question, as researchers have revealed how DNA samples can be potentially falsified.[160] In addition, offenders could plant false DNA evidence at a crime scene.

In any case, while the benefits of DNA profiling and national DNA databases for criminal investigations are clear, both for proving a suspect guilty of a crime or for revealing their innocence, albeit not perfectly, the threat to privacy and liberty is daunting, as DNA collection, storage and analysis becomes more and more common, advanced, revealing, cheaper and easier.

4.6.5 Automatic License Plate Recognition

Automatic License Plate Recognition (ALPR), also known as Automatic Vehicle Identification (AVI), is a mass surveillance technology/system capable of automatically reading or scanning license plates on vehicles and then comparing the number on the license plate with all those stored in databases. An ALPR system is basically made up of cameras, computers and databases. The computers utilize software that manipulates/enhances the images of the license plates and optical character recognition to extract the numbers/letters on the license plate.

ALPR systems are used to identify drivers on the road and locate vehicles that police are searching for. Thus, ALPR systems can potentially offer public security gains in rela-

---

[158] see "Under the Microscope", Her Majesty's Inspector David Blakey, Home Office, July 2000.

[159] House of Commons, Science and Technology Committee, Forensic Science on Trial, Seventh Report of Session 2004-05, para. 62.

[160] see Frumkin, Dan., et al. *Authentication of Forensic DNA samples* (Forensic Science International: Genetics, 2009).

tion to criminal investigations, such as locating a wanted criminal suspect. ALPR systems are also being used in London, for example, to enforce the city's congestion charge.

However, while ALPR systems certainly offer public security gains and other societal benefits, there are legitimate concerns over the capabilities of ALPR systems being used by governments for the general widespread tracking of vehicle movements and other purposes beyond searching for wanted criminal suspects or investigating a crime.

5 BODY SCANNERS: A strip search by other means*

5.1 CHAPTER INTRODUCTION

Since the tragic events of 9/11, the Transportation Security Administration (TSA) has critically served to enhance the ability of airport security screening to detect and/or discover potential threats to aviation security. The deployment of new technology has been central to this enhancement. Body scanners have only recently been deployed at airports across the US as an alternative to patdowns. There are also now calls for their use to eventually replace walk-through metal detectors. Body scanners, however, are highly intrusive upon the privacy of one's body and may violate the Fourth Amendment of the US Constitution, if not proportionally and appropriately used.

Section 5.2 explains the privacy intrusiveness of (backscatter) body scanners, a type of body scanner, comparing them to a strip search. Section 5.3 explains how backscatter body scanners work. Section 5.4 points out their security benefits and drawbacks. Section 5.5 discusses the plausibility of the threat posed by plastic guns, ceramic knives, and liquid/chemical and plastic explosives, which backscatter body scanners are promoted for aiding in their detection or discovery. Section 5.6 describes the possible alternatives to backscatter body scanners in airport security screening.[161] Section 5.7 describes the scope of deployment of body scanners in the US. Section 5.8 outlines the statutory law and case law of special relevance in the US. Section 5.9 evaluates and highlights the deficiencies and dilemmas of the US legal framework in terms of protecting privacy, fulfilling the principles of privacy and upholding the integrity of the Fourth Amendment with regards to the use of body scanners. Section 5.10 outlines some proposals on how to enhance the US legal framework. Section 5.11 briefly explains whether the focus should be on regulating the use or regulating the manufacture

* Chapter 5, despite subsequent additions and modifications, served as the basis for the article I published previously, titled: Backscatter body scanner - A strip search by other means (Computer Law & Security Report, Volume 24, Issue 4, Elsevier, July 2008), pp. 316-325.

[161] This chapter will only discuss the security screening of passengers themselves and not their luggage or carry-on bags.

of body scanners. Section 5.12 outlines the international deployment of body scanners. Section 5.13 ends the chapter with some ending remarks.

5.2 A STRIP SEARCH BY *OTHER MEANS*?

Backscatter body scanners, manufactured by American Science and Engineering, Inc. (AS&E)[162] and Rapiscan (a unit of OSI Systems, Inc.),[163] enable the operator of the device to see just beneath the clothing of an individual, clearly revealing that individual's naked body, including the shape and size of genitals, buttocks and female breasts. As Bill Scannell, a privacy advocate/technology consultant, asserts, "It shows nipples. It shows the clear outline of genitals".[164] Backscatter body scanners can also potentially reveal sensitive medical details about a person, such as mastectomies and colostomy appliances. The graphic anatomical detail of the images produced by backscatter body scanners has led Barry Steinhardt of the American Civil Liberties Union (ACLU) to persistently call their use a "virtual strip search".

As virtual money is used to make payments by other means - electronic means, a virtual strip search is used to inspect one's body by electronic means. But, could a virtual strip search be considered the same as a conventional strip search? Well, society and law enforcement bodies consider virtual money to be just another form of money. Interpol defines virtual money as "an encrypted code representing money, in the same way that paper money is only paper bearing certain characteristics such as graphics and serial numbers".[165] The only main difference is that virtual money is seen on a computer screen. Perhaps, just like virtual/electronic money is increasingly being used in place of conventional paper money and could one day become the dominant medium of exchange, unit of account or store of value in the digital age, virtual strip searches can also substitute conventional strip searches. As William Saletan asserts, "they [backscatter body scanners] don't extend the practice of strip-searching. They abolish it".[166]

---

[162] AS&E, available at: http://www.as-e.com/products_solutions/tsa_z_backscatter_pilot.asp

[163] Rapiscan, available at: http://www.rapiscan.com/sec1000.html

[164] Sharkey, Joe. "Airport Screeners Could Get X-Rated X-Ray Views" (New York Times, 24 May 2005), available at: http://www.nytimes.com/2005/05/24/business/24road.html

[165] Interpol, available at: http://www.interpol.int/Public/TechnologyCrime/CrimePrev/VirtualMoney.asp

[166] Saletan, William. "Naked Came The Passenger" (Washington Post, 4 March 2007), available at: http://www.washingtonpost.com/wp-dyn/content/article/2007/03/02/AR2007030202035_pf.html

Essentially, the only significant difference between the use of backscatter body scanners, without the employment of a privacy algorithm, and the conduct of a conventional strip search is that an individual's naked body is seen not in person, but via a computer screen and without the need to remove a single item of clothing. "Stripping is just a means. Virtual inspections [backscatter body scanners] achieve the same end by *other means*"[167] (emphasis added).

Nonetheless, backscatter body scanners are at present being used as an alternative to patdowns, without the guarantee of the employment of a privacy algorithm. Advocates of backscatter body scanners assert that their use, as an alternative to patdowns, actually enhances the privacy of passengers, since patdowns require physical contact. But, the use of a backscatter body scanner, without the employment of a privacy algorithm, is comparable to conducting a strip search, and thus is considerably more intrusive than an appropriately conducted patdown. Although, according to the TSA, during the trial phase at Sky Harbor International Airport, 70% of passengers opted to be subjected to a backscatter body scanner instead of a patdown,[168] it is unclear whether or not they were fully aware of the intrusive capability of backscatter body scanners or, for instance, if they were shown a true sample of the images generated. Moreover, it was not revealed what percentage of the passengers who opted to be scanned was male or female and it is also unknown how the passengers were surveyed.[169]

In recognition of the intrusive capability of backscatter body scanners and to demonstrate their disapproval of the proposal to deploy them at US airports, Privacy International awarded the Federal Aviation Administration (FAA) the 'Orwell Award' for

---

167 *Ibid.*

168 Frank, Thomas. "Revealing X-ray scanner makes its debut" (USA TODAY, 26 February 2007), available at: http://www.usatoday.com/money/biztravel/2007-02-26-backscatter-usat_x.htm

169 On the other hand, this result was recently confirmed by a more appropriately conducted poll by Gallup. In the midst of the so-called Christmas day attack, 78% of US air travelers surveyed approved of the use of body scanners at US airports. see "In U.S., Air Travelers Take Body Scans in Stride", 11 January 2010, available at: http://www.gallup.com/poll/125018/air-travelers-body-scans-stride.aspx
And even more recently, a survey study conducted by the IT firm Unisys in April 2010, as part of the Unisys Security Index, found that nearly 65% of Americans are willing to undergo full body scans for greater aviation security. see Unisys Press Release available at: http://www.unisys.com/unisys/news/detail.jsp?id=1120000970001910179
But, these results still leave an average of 30% of Americans unwilling to undergo full body scans, which should not be discounted. Moreover, the willingness of US travelers will likely continue to drop as time elapses further away from the so-called Christmas day attack.

the "Most Invasive Proposal".[170] The Electronic Privacy Information Center (EPIC) has equally recognized that body scanners pose a serious threat to privacy and has called for the suspension of the use of body scanners at airports until appropriate laws and regulations are put into place.[171]

5.3 HOW BACKSCATTER BODY SCANNERS WORK

Objects with a high atomic number (high *Z* materials), such as metallic weapons, absorb X-rays, while explosives, containing, for example, nitrogen and carbon, which have a low atomic number (low *Z* materials), scatter X-rays. The intensity of X-ray backscatter decreases as the atomic number (*Z)* increases. Human tissue is predominately composed of oxygen, which has a relatively low atomic number. The technology of backscatter body scanners works by projecting low-radiation X-rays onto an individual while standing in a portal.[172] The X-rays that reflect off the individual or backscatter are detected by the scanner, identified where they came from and converted into a photographic-quality image displayed on a monitor, revealing any concealed objects of low Z material. Backscatter body scanners also recognize the lack of scattering and therefore can reveal any concealed object of high Z material. Concealed objects, both metallic and non-metallic, are distinguishable in backscatter images due to their significant differences in atomic number from human tissue. The image edges of concealed objects of low Z material are ideally enhanced to facilitate their detection.[173]

170 Privacy International, US Big Brother Awards, available at: http://www.privacyinternational.org/bigbrother/us2000 (5 April 2000).

171 Further information is available at: http://epic.org/privacy/airtravel/backscatter/

172 AS&E, available at: http://www.as-e.com/products_solutions/smart_check.asp

173 see World Intellectual Property Organization, International Application No.: PCT/US1991/005558, Publication No.: WO/1992/002937, Publication Date: 20 February 1992, Applicant: IRT CORPORATION, available at: http://www.wipo.int/pctdb/en/wo.jsp?IA=WO1992002937&DISPLAY=DESC;
U.S. Patent No. 7,110,493, entitled "X-ray detector system having low Z material panel", Issued to Rapiscan Security Products, Inc. on September 19, 2006.

5.4 SECURITY BENEFITS AND DRAWBACKS OF BACKSCATTER BODY SCANNERS

Evidently, there are systemic vulnerabilities in the security screening process at airports. This is true not just in the US, but internationally. The covert security audits, conducted by the TSA and the GAO, have especially revealed the vulnerabilities at US airports. GAO investigators managed to get though airport security checkpoints undetected with either improvised explosive devices (IEDs) or improvised incendiary devices (IIDs) hidden both in their carry-on luggage and on their persons.[174] In 2007, it was publicly disclosed that TSA screeners on numerous occasions failed to detect simulated explosives and bomb parts hidden under the clothes of TSA covert security auditors.[175] A few months later, it was reported that a loaded firearm slipped through airport security[176] and a TSA screener, during a covert security audit, failed to detect a fake bomb even after conducting a patdown.[177]

While the vulnerabilities are partly due to "human factors",[178] the main problem, in the first place, is the incapability of walk-through metal detectors (WTMDs) to detect plastic guns, ceramic knives, and liquid/chemical and plastic explosives. The other significant problem is with patdowns. The quality of patdowns may vary significantly, due to human factors, and patdowns cannot reveal relatively small amounts of chemical or plastic explosives hidden very close to a person's genitals, such as within their underwear,

[174] see Aviation Security: Vulnerabilities Exposed Through Covert Testing of TSA's Passenger Screening Process, Statement of Gregory D. Kutz, Managing Director Forensic Audits and Special Investigations, and John W. Cooney, Assistant Director, Forensic Audits and Special Investigations of the United States Government Accountability Office, during the testimony before the Committee on Oversight and Government Reform, House of Representatives, 15 November 2007, available at: http://oversight.house.gov/documents/20071114175647.pdf

[175] Frank, Thomas. "Most fake bombs missed by screeners" (USA TODAY, 17 October 2007), available at: http://www.usatoday.com/news/nation/2007-10-17-airport-security_N.htm

[176] see "Loaded gun slips through airport security" (CNN, 23 January 2008), available at: http://edition.cnn.com/2008/US/01/23/airport.gun/index.html

[177] see "TSA tester slips mock bomb past airport security" (CNN, 28 January 2008), available at: http://edition.cnn.com/2008/US/01/28/tsa.bombtest/index.html

[178] "Human factors" refers to the demands a job places on the capabilities of, and the constraints it imposes on, the people doing it. For screeners, the human factors issues cited in past studies include the repetitive tasks screeners perform, the close and constant monitoring required to spot the rare appearances of dangerous objects, and the stress involved in dealing with the public, who may dislike being screened or demand faster action to avoid missing their flights". U.S. General Accounting Office, Aviation Security: Long-Standing Problems Impair Airport Screeners' Performance, GAO/RCED-00-75 (Washington, D.C.: 28 June 2000), p. 26.

since patdowns conducted at airports in the US and in Europe do not normally involve the touching of these sensitive areas. While the deficiencies of WTMDs and patdowns were always clear to security experts, these deficiencies have been especially highlighted by the so-called "underwear bomb" containing PETN (pentaerythritol tetranitrate) that made it through Amsterdam's Schiphol Airport undetected on December 25, 2009.

Indeed, backscatter body scanners can (potentially) significantly enhance the security screening process at airports and reduce the adverse effects of human factors by facilitating security screeners to detect or discover any object hidden on a person that metal detectors and sometimes a patdown cannot or do not.[179]

Nevertheless, like any single security apparatus, device or system, (backscatter) body scanners are certainly not foolproof. Since the low-radiation X-rays emitted from backscatter body scanners only penetrate about 0.1 inches (0.254 centimeters) of the skin, they are unable, for instance, to reveal threats hidden deeper in body cavities. Terrorists determined to get pass security screening with a bomb, for example, can hide explosives and a detonator in their rectum, which was indeed the new strategy reportedly used by al Qaeda to target Saudi Prince Mohammed Bin Nayef inside a palace in August 2009.[180] There is also a risk from high-explosives surgically implanted within skin tissue, where they may potentially not be revealed by body scanners, for example under breast tissue.[181] In addition, body scanners apparently may also have potential difficulties in detecting

[179] During the second meeting of the Task Force on Security Scanners in 2010, first set up by the European Commission, representatives present from Schiphol Airport, Manchester Airport and the UK Department of Transport, for instance, explained that after their trial phases of body scanners, they are convinced that the evidence proves that body scanners offer immense security benefits and enhancements (i.e. improved detection of both metallic and non-metallic threats on a person). The European Commission has equally recognized and acknowledged the security benefits of body scanners, which must be seriously taken into consideration. see the Communication from the Commission to the European Parliament and the Council on the Use of Security Scanners at EU airports (COM(2010) 311 final), 15.6.2010.

[180] MacVica, Sheila. "Al Qaeda Bombers Learn from Drug Smugglers: New Technique of Storing Bomb Materials Inside Body Cavity Nearly Kills a Saudi Prince" (CBS News, 28 September 2009), available at: http://www.cbsnews.com/stories/2009/09/28/eveningnews/main5347847.shtml

[181] Reportedly, terrorists are known to have implanted PETN in the breasts of women. see "Terrorists Could Use Explosives in Breast Implants to Crash Planes, Experts Warn" (The Sun, 24 March 2010), available at: http://www.foxnews.com/world/2010/03/24/terrorists-use-explosives-breast-implants-crash-planes-experts-warn/?test=latestnews

explosives hidden in shoes or items stitched into clothing.[182] The security vulnerabilities of body scanners were additionally highlighted by the GAO in a 2009 report[183] and again most recently in a report released in 2010.[184] Hence, the reason why a "holistic approach" is required for ensuring aviation security, as the European Commission argues, which embodies a combination of a variety of devices and methods.[185]

On a different note, the non-security related drawbacks of backscatter body scanners include the requirement of up to 45 seconds to completely scan a passenger, and therefore backscatter body scanners may hinder the flow of passengers.[186]

5.5 THE PLAUSIBILITY OF THE THREAT POSED BY PLASTIC GUNS, CERAMIC KNIVES, AND LIQUID/CHEMICAL AND PLASTIC EXPLOSIVES

Since the privacy intrusion should match the threat for which it aims to prevent or address, in accordance with the *principle of proportionality*, those threats themselves should be evaluated and explained.

First of all, there is no evidence that guns completely made of plastic, including ammunition, exist. Even if they do exist, it is highly doubtful terrorists could get their hands on one. A Glock is probably the closest known weapon to a plastic gun, made of

182 Jonathan Corbett, an engineer and blogger, has published a video showing how he managed to go through a backscatter body scanner without the system detecting a small metal case that was stitched into a special side pocket of the shirt he was wearing. YouTube is understandably restricting access to the videos. As the UK Daily Mail reports, he suggests that this is because the body scanners "blend metallic areas into the dark background – so if an object is not directly placed on the body, it will not show up on the scan". see Moran, Lee. "How to get ANYTHING through TSA nude body scanners: Blogger exposes loophole in $1billion fleet" (7 March 2012), available at: http://www.dailymail.co.uk/news/article-2111417/TSA-nude-body-scanners-Jonathan-Corbett-video-exposes-loophole.html#ixzz1oRILtdLo

183 see Aviation Security: DHS and TSA Have Researched, Developed, and Begun Deploying Passenger Checkpoint Screening Technologies, but Continue to Face Challenges, GAO-10-128, 7 October 2009, available at: http://www.gao.gov/new.items/d10128.pdf

184 see Homeland Security: Better Use of Terrorist Watchlist Information and Improvements in Deployment of Passenger Screening Checkpoint Technologies Could Further Strengthen Security, GAO-10-401T, 27 January 2010, available at: http://www.gao.gov/new.items/d10401t.pdf

185 Communication from the Commission to the European Parliament and the Council on the Use of Security Scanners at EU airports (COM (2010) 311 final), 15 June 2010.

186 Wilber, Del Quentin. "Airport Security Technology Stuck In the Pipeline" (Washington Post, 8 February 2008), available at: http://www.washingtonpost.com/wp-dyn/content/story/2008/02/07/ST2008020704150.html

83% steel by weight, but it is clearly detectable by metal detectors. Besides, the manufacture of plastic guns or any other undetectable firearm, which has less than 3.7 ounces of metal, has been banned in the US since 1988.[187] However, the law explicitly does not ban the manufacture of such weapons exclusively for US military or intelligence agencies, and nor does it prevent their possible manufacture in other countries.[188]

The threat posed by ceramic knives, which have blades made from zirconia and handles made from nylon, has been exaggerated, to some extent, and is certainly not serious enough to merit the widespread use of backscatter body scanners, regardless if ceramic knives are even harder and can remain sharper than steel knives. Although terrorists managed to hijack airplanes using only box cutters and then tragically crash the airplanes into buildings on 9/11, today reinforced cockpit doors are securely locked throughout flights, as required by law.[189] In addition, the Aviation and Transportation Security Act of 2001 (ATSA) sanctioned the expansion of the federal air marshal service[190] and authorized pilots to carry firearms.[191] However, a recent CNN nationwide investigation revealed that only an estimated 1% of commercial airline flights on a daily basis are in fact protected by armed federal air marshals and field offices are increasingly shorthanded.[192]

There are threats posed by liquid/chemical explosives carried on a person onboard an airplane. But, these threats vary in degree, depending on the type of liquid/chemical explosive. On August 10, 2006, an apparent terrorist plot to blow up airplanes, reportedly using triacetone triperoxide (TATP) made onboard, was thwarted in the UK.[193] This led to restrictions on bringing any type of liquid onboard airplanes. TATP is a liquid explosive composed of hydrogen peroxide, sulfuric acid and acetone, each essentially innocuous to aviation security on their own, but explosive when mixed together. Although

187 An Act to reauthorize the ban on undetectable firearms (Public Law 108-174), which reauthorized for a further ten years the Undetectable Firearms Act of 1988 (Public Law 100-649).

188 *Ibid.*

189 Aviation and Transportation Security Act of 2001 (Public Law 107-71), SEC. 104.

190 *Ibid.*, SEC. 105.

191 *Ibid.*, SEC. 128.

192 Griffin, Drew., Kathleen Johnston and Todd Schwarzschild. “Sources: Air marshals missing from almost all flights” (CNN, 25 March 2008), available at: http://www.cnn.com/2008/TRAVEL/03/25/siu.air.marshals/index.html

193 see Laville, Sandra., Richard Norton-Taylor and Vikram Dodd. “A plot to commit murder on an unimaginable scale” (The Guardian, 11 August 2006), available at: http://www.guardian.co.uk/uk/2006/aug/11/politics.usa1

TATP is indeed explosive, with power close to that of TNT,[194] the implausibility lies in the immense difficulty of mixing the chemical ingredients onboard an airplane, without the proper apparatus and the necessary low temperature conditions, while managing not to alert other passengers in the process.[195] In addition, before TATP can be detonated it must first crystallize out of solution, which can take hours, and a considerable amount is required to bring down an airplane.[196] Instead of making TATP onboard an airplane, the explosive could be carried onboard, undetected by conventional methods of screening, given that it contains no nitro groups or metallic elements.[197] However, TATP is one of the most unstable explosives known[198] and thus it is likely to detonate prematurely when carried on a person, i.e. before boarding an airplane.

There are numerous other explosives in liquid form, such as nitroglycerin, nitromethane and Astrolite G, a mixture of ammonium nitrate and hydrazine. But, these compounds also present difficulties for terrorists. Nitromethane gives off a very pungent smell, which would likely alert airport screeners, nitroglycerin is highly unstable and a noticeable amount would be required to bring down an airplane, and hydrazine is extremely toxic and corrosive. But, these challenges and hazards might not be enough to deter terrorists, and additional methods, beyond those discussed here, for developing liquid or chemical explosives are certainly possible.

Other explosives that pose a considerable more serious threat to commercial aviation security include plastic explosives, such as C-4, PE4, Semtex, PETN and polymer-bonded explosives (PBX). These explosives are ready for detonation, undetectable to metal-detectors, generally odorless and only a relatively small amount is required to bring down an airplane. PETN was the explosive used by Umar Farouk Abdulmutallab, which he hid in his underwear and managed to get through security at Amsterdam's Schiphol Airport undetected, in order to attempt to destroy a Northwest Airlines aircraft on December 25, 2009 (known as the "Christmas Day attack"). It was also reportedly

---

194 see Dubnikova, Faina., et al. Decomposition of Triacetone Triperoxide Is an Entropic Explosion (Journal of the American Chemical Society, January, 2005), p. 1, available at: http://www.technion.ac.il/~keinanj/pub/122.pdf

195 see Greene, Thomas C. "Mass murder in the skies: was the plot feasible?" (The Register, 17 August 2006), available at: http://www.theregister.co.uk/2006/08/17/flying_toilet_terror_labs/print.html; *Perks, Bea.* and *Katharine Sanderson.* "Terror plot sparks frenzied speculation about liquid explosives" (The Royal Society of Chemistry, 11 August 2006), available at: http://www.rsc.org/chemistryworld/News/2006/August/11080602.asp

196 see *Ibid.*

197 see Dubnikova, Faina., et al, 2007.

198 *Ibid.*

the same type of explosive molded into the soles of the shoes of Richard Reid in an attempt to destroy an American Airlines aircraft around eight years earlier.

5.6 ALTERNATIVES TO BACKSCATTER BODY SCANNERS

The security checkpoint at airports is essentially the last layer of security or defense in commercial aviation, besides the strategic placement of Federal Air Marshals onboard airplanes, the mighty capabilities of the US Air Force and NORAD, and technical countermeasures against shoulder-fired missiles. Before passengers reach security checkpoints, there are a number of additional security measures taken. Passengers are required to submit accurate and thorough personal data when reserving an airline ticket and are profiled or pre-screened against a terrorist watch list maintained by the TSA. Passengers are also required to present a passport or ID card before boarding and these identity documents are checked for authenticity. Passports and ID cards from around the world are increasingly becoming more sophisticated and difficult to forge, albeit certainly not impossible. Bomb-sniffing dogs are also important and are used at airports across the US. Other methods of passenger screening include Screening of Passengers By Observation Techniques (SPOT), whereby TSA officers, known as Behavior Detection Officers (BDOs), are specially trained to look for subtle suspicious indicators, such as particular facial gestures, in what is known as micro-expression training. Finally, domestic and foreign (human) intelligence is certainly also a critical factor, if not the most critical, in discovering a terrorist plot and preventing its execution.

Although technology is just one element of ensuring aviation security and for screening passengers at airport security checkpoints, it is considered key to the development of the so-called “checkpoint of the future”. The development, testing and deployment of technological equipment, which detects explosives in all forms, chemical/biological weapons and non-metallic weapons, is mandated as a “high priority” for the DHS.[199] Technology has consistently been considered critical for ensuring aviation security. For instance, from 2003-2004, the TSA and the DHS funded over 200 R&D projects with the aim of developing technologies for enhancing the security of transportation, particularly in aviation.[200] In 2004, the TSA spent 79.5% of its $159 million

---

[199] see Title 49 U.S.C, Subtitle VII, Part A, Subpart III, Chapter 449, Subchapter I, Section 44925(a).

[200] see US Government Accountability Office, Transportation Security R&D: TSA and DHS are Researching and Developing Technologies, but Need to Improve R&D Management, GAO No. 04-890, 2004, available at: http://www.gao.gov/new.items/d04890.pdf

transportation security R&D budget on researching and developing aviation security technologies and the DHS spent 71.9% of its $88 million R&D budget for the same purposes.[201] And, this is just a fraction of the total amount of money the US Government has spent on procuring aviation security technologies.

The technological alternatives to backscatter body scanners, discussed below, are other devices that can also facilitate the detection of threats hidden on a person during the passenger screening process. With the exception of active millimeter wave portals, several of these alternatives are considerably more privacy-friendly, yet still capable of helping to ensure aviation security. However, arguably none of these alternative devices or technologies are foolproof either.

Active millimeter wave portals, prominently manufactured by L-3 Communications, are another type of body scanner. They are also being piloted or deployed at numerous airports and other locations across the US. Rather than low dose X-rays, extremely high radio frequency (RF) energy/waves is projected onto the body's surface, rendering clothes lucent, and an image is created from the radio waves reflected. Therefore, similar to backscatter body scanners, active millimeter wave portals can practically see through clothes and can potentially reveal concealed metallic or non-metallic threats. Millimeter wave portals, however, may require less time to scan each passenger. But, the ability of millimeter wave portals to detect low-density objects or materials, such as chemical or liquid explosives, is not certain and has been called into question. Another drawback is that airport screeners may likely require additional specific training in order to correctly analyze the active millimeter wave images.

While the images produced by active millimeter wave portals are different from the images produced by backscatter body scanners and appear to be not as graphically detailed, active millimeter wave portals are still highly privacy-intrusive, essentially equal to that of backscatter body scanners, and certainly considerably more intrusive than ordinary patdowns. Active millimeter wave portals gained popularity over backscatter body scanners not because they are more privacy-friendly, but rather because they do not project X-rays, which is a publicized concern of passengers.

Millivision's Automatic Threat Detection (ATD) System uses passive millimeter wave imaging technology, as opposed to active millimeter wave imaging technology. The system detects and distinguishes the millimeter wave energy that is naturally emitted from a person's body from the wave energy emitted from objects hidden under a

[201] *Ibid*., p. 4 and p. 22. However, this funding is not only for checkpoint security or passenger/luggage screening, and includes the CAPPS II program and technical countermeasures for defending against shoulder-fired missiles.

person's clothes and then generates an image, which can potentially help to discover any concealed object.[202]

Combining digital video recorders with passive millimeter wave imaging technology, Brijot's BIS-WDS® GEN 2 is also capable of screening passengers for both concealed metallic and non-metallic weapons and explosives, but fully avoids the privacy concern of seeing through clothes by neither generating an anatomically detailed image nor absolutely requiring security officers to monitor the images. An on-board computer comprised of an "intelligent detection engine" can (potentially) pinpoint in real-time the location of potential threats on any person, whether still or moving, who enters the system's "field of view" and automatically alert security officers.[203] Brijot's system can examine a person in as little as 0.5 seconds and therefore does not slow down at all the flow of passengers.[204] Brijot's BIS-WDS® GEN 2 is much like Rapiscan's WaveScan 200, which also uses passive millimeter wave technology. The intelligent detection engine, however, likely requires further development and validation in order to be assured of its effectiveness. Brijot's SafeScreen is another privacy-friendly alternative, whereby metals, plastics, ceramics, composites, liquids, gels, explosives, etc. can be discovered on a person by detecting and showing objects that are colder or hotter than the surface temperature of the subject, also without generating an anatomically detailed image. Brijot is marketing these devices as means for primary security screening at airports and other locations.

ThruVision has also developed similar imaging technology. The T5000 passive terahertz imaging system is equally capable of revealing both metallic and non-metallic objects hidden under clothing on multiple still or moving persons some distance away. Terahertz rays or T-rays are a form of low-level radiation, between infrared light and microwaves on the electromagnetic spectrum, and are naturally emitted from all materials. The T5000 works by collecting the T-rays emitted off a person and processing them to form images that reveal any concealed objects, also without displaying physical details of the body.[205] Picometrix also develops similar terahertz imaging technology.

---

202 Millivision, available at: http://www.millivision.com/technology.html

203 The technology, however, still requires further advancement in order to be a trustworthy replacement of well-trained screeners, as pointed out by *Eckard Seebohm*, Head of the Aviation Security Unit of the European Commission during the first Body Scanners Task Force public consultation meeting held on 12 December 2008 at the Centre Albert Borschette in Brussels.

204 Brijot, available at: http://www.brijot.com/products/BIS-WDS_Gen2

205 ThruVision, Press Release (7 March 2008), available at: http://www.thruvision.com/images/PDFs/News/thruvision%20introduces%20t5000.pdf

The SPO camera units, developed by QinetiQ also use passive millimeter wave technology to detect the waves naturally emitted by the human body and to determine if there are any "cold" objects, such as metals, plastics and ceramics concealed under a person's clothing. Suspicious objects are meant to trigger a red light on the display monitor, prompting the operator to search the individual. SPOs do not rely on image screening and can rapidly scan people simultaneously as they are moving, thereby neither producing still nor revealing images. The TSA deployed SPO camera units at the Denver International Airport during the 2008 Democratic National Convention.[206]

While passive millimeter wave technology and the BIS-WDS® GEN 2, T5000 and SPO are viable and privacy-friendly alternatives to backscatter body scanners, they are also not yet as sophisticated and especially do not generate images that are clear or detailed enough to offer the same degree of security benefits of active millimeter wave portals or backscatter body scanners.[207] Moreover, these alternatives still require further testing and operational trials. For now, the TSA is testing passive millimeter technology at Boston's Logan International Airport, and the technology is also being tested in the UK.

Alternatives to advanced imaging technologies include the explosive trace detection (ETD) technology of General Electric's EntryScan, which is a trace portal machine (also known as a "puffer machine"). EntryScan works on the premise that when a terrorist prepares an explosive device tiny amounts of the explosive materials get on their skin, clothes or hair. When a person steps into the gateway of an EntryScan, air is blasted onto that person and the tiny particles that are liberated are collected and instantly analyzed for explosive chemicals. This screening methodology probably does not raise any privacy concerns. However, an obvious drawback with puffer machines is that they are not reliable if a terrorist has worn a full protective suit when preparing the explosive device concerned and has tightly sealed it in plastic. Puffer machines have been deployed in airports across the US, but they are currently being phased out due to maintenance issues and problems caused by dust and dirt continuously breaking down the machines.[208]

Other non-invasive ETD technologies or methods include the use of portable or stationary 'swabbing devices' that are able to detect explosive chemicals on a per-

---

[206] QinetiQ, "US Transportation Security Administration Deploys QinetiQ New Airport Security Technology", 4 September 2008, available at: http://www.qinetiq.com/home/newsroom/news_releases_homepage/2008/3rd_quarter/spo_at_us_conventions.html

[207] This representatives from Schiphol Airport pointed this out during the first Body Scanners Task Force public consultation meeting held on 12 December 2008 at the Centre Albert Borschette in Brussels. The meeting was chaired by *Eckard Seebohm*, Head of the Aviation Security Unit of the European Commission.

[208] see Tessler, Joelle and Arthur Max. "Better airport scanners delayed by privacy fears" (Associated Press, 28 December 2009).

son's hands or on his or her hand bags. Thousands of these devices have already been deployed at US airports and the TSA has begun to randomly select people for hand swabbing. The devices can be used not just at security checkpoints, but also throughout an airport including at boarding gates. There are, however, also drawbacks with these devices. Legal and non-threatening substances could potentially result in 'false positives'[209] and 'false negatives' could result when a terrorist has successfully managed to completely avoid touching the hidden explosive.

Ahura Scientific's FirstDefender is a hand-held device that uses a method of analysis called raman spectroscopy to detect explosives or other chemicals in sealed plastic or glass containers. The FirstDefender works by projecting a laser beam onto the unknown solid or liquid substance and analyzing the light that scatters back to the device. Every substance scatters light in a unique way and the FirstDefender can determine the scattering patterns of a vast array of explosives, toxic industrial chemicals, toxic industrial materials and chemical warfare agents.[210] The most serious drawback is that the FirstDefender cannot analyze substances in non-translucent containers or those hidden underneath clothes and a considerable amount of the substance is required. Prospective advancements in raman spectroscopy, known as Surface Enhanced Raman Spectroscopy (SERS), can incredibly enhance the sensitivity of this explosive detection technique, but the technology is still in its early stages.[211]

On the other hand, the Fido® PaxPoint™, a handheld device developed by ICx Technologies, is capable of detecting liquids used in making explosive devices in both clear and opaque containers by analyzing vapors emitted from the bottle's opening.[212] The TSA is piloting the device.

The GK1, developed by Nemesysco, uses Layered Voice Analysis (LVA) technology to determine in advance the real intentions of people and to conduct a threat assessment by using input from 3-5 questions. The GK1 is like a lie detector. LVA uses signal-processing algorithms that can differentiate between a "normal" voice and a "stressed" voice. If the GK1 detects stress, security personnel can take the concerned person aside

---

209 Meserve, Jeanne., and Mike M. Ahlers. "TSA to swab airline passengers' hands in search for explosives" (CNN.com, 17 February 2010), available at: http://www.cnn.com/2010/TRAVEL/02/17/tsa.hands.swabbing/index.html

210 Ahura Scientific, available at: http://www.ahurascientific.com/chemical-explosives-id/products/firstdefender/index.php#

211 see Hambling, David. "Army Seeks Super-Sniffer to Detect Explosives, Bio-Agents" (Wired Magazine, 10 September 2009), available at: http://www.wired.com/dangerroom/2009/09/army-seeks-super-sniffer-to-detect-explosives-bio-agents/

212 ICX Technologies, available at: http://www.icxt.com/products/icx-detection/explosives/fido-paxpoint/

for further questioning and a patdown. The system is based on the premise that all voices have a certain frequency and any deviation from that frequency can indicate an increase in stress, excitement or anticipation. The GK1 has been tested at Moscow Domodedovo International Airport.[213] The GK1 is part of the growing movement towards using biometric sensors at airports to measure the body temperature, respiration and heart rate of passengers, which can be potentially used to determine their intentions or state of mind. However, voice analysis or other biometric sensors might not work on hardened terrorists that are neither physically nor emotionally affected by their mission. Moreover, the GK1 could unnecessarily subject people who are just naturally stressed and nervous to thorough questioning or a patdown by security personnel. The technology, however, is also not yet sophisticated enough.

A potential technological alternative to deploying new explosive detection devices or advanced imaging technologies is perhaps the comprehensive improvement of the PNR system and the requirement of additional personal data from passengers, including the more effective use of that data. In this case, more data protection rights may be sacrificed for greater corporeal privacy.

5.7 SCOPE OF DEPLOYMENT IN THE US

Backscatter technology has been around for decades, however, only recently has the US Government officially authorized the expansion of backscatter technology onto passenger screening and appropriated extensive funding to do so.[214] Even before that, the US Government provided the necessary R&D funding for advanced X-ray screening systems for individuals.[215]

Backscatter body scanners have reportedly been either piloted or fully deployed at dozens of major international airports across the US, including: O'Hare in Chicago; JFK in New York; LAX in Los Angeles; Miami International Airport; Hartsfield-Jackson in Atlanta; George Bush International Airport in Houston; Dulles International

213 Nemesysco, available at: http://security.nemesysco.com/gk1.html

214 see Intelligence Reform and Terrorism Prevention Act of 2004 (Public Law 108-458), SEC. 4013.

215 see HR 1271, "FAA Research, Engineering, and Development Authorization Act of 1997" (Public Law No: 105-155)

Airport; and Sky Harbor International Airport in Phoenix, Arizona.[216] Backscatter body scanners are also being used in several prisons in the US[217] and reportedly other domestic locations.

In the US, as of November 2009, according to the TSA and what has been reported, 46 backscatter body scanners were piloted at 23 airports, and 40 millimeter wave portals have been deployed at 19 airports. Six airports are using the advanced imaging technology for primary screening, rather than as an alternative to a patdown for secondary screening.[218]

The TSA earlier on announced plans to deploy an additional 150 <u>backscatter</u> body scanners beginning 2010, already purchased from Rapiscan in 2009, at airport security checkpoints across the US and use them to <u>replace</u> WTMDs.[219] And, as a consequence of Umar Farouk Abdulmutallab's attempt to destroy a Northwest Airlines aircraft on December 25, 2009, using PETN hidden in his underwear and undiscovered by a patdown, the deployment of body scanners will only increase.[220] Already the US Secretary for Homeland Security, Janet Napolitano, has announced that an additional 300 body

---

216 US Customs TODAY, March 2000, available at: http://www.cbp.gov/custoday/mar2000/bodyscan.htm; Frank, Thomas. "TSA looks into using more airport body scans" (USA TODAY, 7 October 2007), available at: http://www.usatoday.com/news/washington/2007-10-07-backscatter_N.htm; Frank, Thomas. "Air travelers stripped bare with X-ray machine" (USA Today, 15 May 2005), available at: http://www.usatoday.com/news/nation/2005-05-15-airport-xray-bottomstrip_x.htm
Other airports in the US where body scanners have been deployed include: Albuquerque International Sunport Airport; Baltimore/Washington International Thurgood Marshall Airport; Bob Hope Airport; Cleveland Hopkins International Airport; Denver International Airport; Detroit Metro Airport; Indianapolis International Airport; Jacksonville International Airport; McCarran International Airport; Raleigh-Durham International Airport; Richmond International Airport; Rochester International Airport; Ronald Reagan Washington National Airport; San Francisco International Airport; Salt Lake City International Airport; Tampa International Airport; Tulsa International Airport. see http://www.tsa.gov/approach/tech/imaging_technology.shtm, last visited 12/11/09.

217 Presidential Report on Radiation Protection Advice: Screening of Humans for Security Purposes Using Ionizing Radiation Scanning Systems (National Council on Radiation Protection and Measurements, 2003), p. 16, Section 3.1.1, available at: http://www.fda.gov/ohrms/dockets/ac/03/briefing/3987b1 pres-report.pdf

218 see http://www.tsa.gov/approach/tech/imaging_technology.shtm

219 Frank, Thomas. "TSA to expand use of body scanners" (USA Today, 1 October 2009), available at: http://www.usatoday.com/tech/news/surveillance/2009-09-30-backscatter-body-scanners_N.htm

220 In acknowledging that the deployment of body scanners will likely increase, the stock market shares for the manufacturers of body scanners surged during the aftermath of the Christmas Day attack (particularly more so for backscatter body scanners). By January 11 2010, the shares of OSI Systems, Inc. (NASDAQ:OSIS) (parent company of Rapiscan), for example, jumped nearly 50%, from around $22 to around $32 a share.

scanners will be deployed in 2010.[221] That makes a total of 450 additional body scanners planned for deployment in 2010.[222] Furthermore, the Obama Administration revealed their proposed budget for 2011 (fiscal year October 2010-September 2011), subject to congressional approval, which allocates a whopping $734 million for Advanced Imaging Technology (AIT) and the procurement of 1,000 additional body scanners. However, at around $150,000 each, this funding would be sufficient to procure over 4,000 body scanners, which is more than enough to deploy body scanners at practically every airport security checkpoint in the US, with extra for airports outside the US.

On the other hand, none of the 150 backscatter body scanners purchased by the US Government in 2009 and delivered by Rapiscan have yet to be deployed and are currently (as of February 2010) reportedly still sitting in storage,[223] but reportedly will be swiftly deployed.

5.8 LAWS, CODES AND OTHER LEGAL/POLICY INSTRUMENTS OF SPECIAL RELEVANCE IN THE US

In the US, as a common law country, case law and judicial interpretations of the Fourth Amendment of the US Constitution play a particularly important role. The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

221 Weisman, Jonathan and Siobhan Gorman. "Obama orders security fix" (The Wall Street Journal, 8 January 2010), available at: http://online.wsj.com/article/SB126287015166119561.html?mod=article-outset-box

222 see the written statement of Secretary of Homeland Security Janet Napolitano for a hearing entitled "The State of Aviation Security - Is Our Current System Capable of Meeting the Threat?" before the US Senate Committee on Commerce, Science, and Transportation, 20 January 2010.

223 see Jack Cafferty, Gov't hasn't installed one airport scanner with stimulus $$$, Cafferty File, CNN.com, 23 February 2010, available at: http://caffertyfile.blogs.cnn.com/2010/02/23/govt-hasnt-installed-one-airport-scanner-with-stimulus/

The Fourth Amendment gives individuals freedom from any unreasonable search and seizure conducted by the US Government and has significantly served as the basis of the right to privacy in the US, but is not explicitly a constitutional right to privacy *per se*.

As the US Supreme Court affirms "[t]he overriding function of the Fourth Amendment is to protect personal privacy and dignity against unwarranted intrusion by the State".[224] At first, this was limited to physical intrusions upon a person's property.[225] However, adapting to technological advancements, the US Supreme Court in *Katz v. United States* later extended the interpretation of the Fourth Amendment to include not just properties or physical places, but also people,[226] as long as the person concerned exhibits first "an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as reasonable".[227] This condition formulated by Justice Harlan is commonly known as the *Katz* test or the Harlan standard. The Fourth Amendment furthermore requires that the US Government "accept as axiomatic the principle that people harbor a reasonable expectation of privacy in their 'private parts".[228]

In *Kyllo v. United States*, the US Supreme Court held that the use of a thermal imaging device to search for evidence in the interior of a home through its walls, which would otherwise not be possible without physically entering the home, constituted a search for the purposes of the Fourth Amendment and was unreasonable and thus unconstitutional without a warrant.[229] In addition, the US Supreme Court based its judgment on the potential of thermal imaging to reveal intimate details.[230] If the same legal reasoning is applied, the use of fully-intrusive backscatter body scanners to peer through an individual's clothes, revealing intimate details, which would otherwise not be possible without physically removing that individual's clothes, may also constitute a search for the purposes of the Fourth Amendment (Minert, 2006).

The US Supreme Court in *Terry v. Ohio* held that a warrantless search for weapons by a law enforcement officer is constitutional if it is "strictly circumscribed by the exigencies

---

224 *Schmerber v. California,* 384 U.S. 757, 767 (1966).

225 see *Olmstead v. United States*, 277 U.S. 438 (1928).

226 see *Katz v. United States*, 389 U.S. 347, 351 (1967).

227 *Ibid.*, at 361. Concurring opinion of Justice Harlan.

228 *Justice v. City of Peachtree City*, 961 F.2d 188, 191 (11th Circuit, 1992).

229 see *Kyllo v. United States*, 533 U.S. 27 (2001).

230 *Ibid.*

which justify its initiation" and "limited to that which is necessary for the discovery of weapons which might be used to harm the officer or others nearby, and may realistically be characterized as something less than a "full" search, even though it remains a serious intrusion".[231] The 4th Circuit, just several years later, extended the reasoning of the US Supreme Court in *Terry v. Ohio* to justify airport searches using magnetometers to search for weapons in order to prevent the hijacking of airplanes and the subsequent physical "frisk", depending on the information provided by the magnetometer.[232]

Although the Fourth Amendment prohibits "unreasonable searches", it nonetheless does not necessarily signify a warrant is required for all searches. Indeed, what the Fourth Amendment explicitly requires is that searches are "reasonable". If the search is reasonable, then it is constitutional and, therefore, lawful.[233]

While all passengers must be searched before boarding an airplane, it is widely recognized that the conduct of any border search must therefore still be reasonable and in accordance with the Fourth Amendment.[234] Privacy does not just vanish at borders and US Customs agents or airport screeners are not given a blanket license to intrude upon the privacy of individuals. For instance, the limited right to privacy at airports does not entail that passengers can be strip searched without grounds of reasonable suspicion, regardless of the legitimate public interests. As the 9th Circuit Court affirmed, "exercise of the constitutional right to travel may not be conditioned upon the relinquishment of another constitutional right [i.e. the Fourth Amendment] […]".[235]

The US Supreme Court has provided the preliminary grounds to determine if a search is reasonable. To determine its "reasonableness," "the scope of the particular intrusion, the manner in which it is conducted, the justification for initiating it, and the place in which it is conducted" must be considered.[236] As the 5th Circuit Court in *United States v. Skipwith* affirmed, to determine the reasonableness of a border search the fol-

---

231 *Terry v. Ohio*, 392, U.S. 1, 26 (1968).

232 *United States v. Epperson*, 454 F.2d 769 (4th Circuit, 1972).

233 For further discussion, see Vina, Stephen R. *Virtual Strip Searches at Airport: Are Border Searches Seeing Through the Fourth Amendment?* (8 Texas Wesleyan Law Review, 2001-2002), pp. 417-439; Mock, Tobias W. The TSA's New X-Ray Vision: *The Fourth Amendment Implications of "Body Scan" Searches at Domestic Airport Security Checkpoints* (49 Santa Clara Law Review, 2009), pp. 213-252.

234 see, e.g., *Marsh v. United States*, 344 F.2d 317 (5th Circuit, 1965); *United States v. Montoya de Hernandez*, 473 U.S. 531 (1985); *United States v. Skipwith*, 482 F.2d 1272 (5th Circuit, 1973) at 1276.

235 *United States v. Davis*, 482 F.2d 893, 913 (9th Circuit, 1973).

236 *Bell v. Wolfish*, 441 U.S. 520, 559 (1979).

lowing three factors must be considered: "public necessity, efficacy of the search, and degree of intrusion […]".[237] The US Supreme Court, in another case several decades later, held that the reasonableness of a search can be determined "by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of a legitimate governmental interests".[238] Aviation security is undoubtedly considered a legitimate public (or governmental interests) and searches at airport security checkpoints undoubtedly play a critical role in ensuring aviation security.

US Customs agents or other authorized government officials are legally permitted to conduct searches of individuals at borders without a warrant.[239] This is commonly known as the "border search exception". Warrantless border searches are also deemed reasonable and acceptable under the Fourth Amendment since they occur at a border[240] and have long been considered necessary in order for a state to protect itself and ensure legitimate governmental interests.[241] US courts have firmly established that "the Fourth Amendment's balance of reasonableness is qualitatively different at the international border than in the interior".[242] Airports located anywhere within the US act as the "functional equivalent of the border".[243] Moreover, it would obviously be impractical or unrealistic for the TSA to require a warrant to carry out airport security screening.[244]

Border searches are divided into routine and non-routine. Routine border searches do not require reasonable suspicion to be carried out since they are minimally intrusive.

---

237 *United States v. Skipwith*, 482 F.2d 1272, 1275 (5th Circuit, 1973); see Minert, Steven R. S*quare Pegs, Round Hole: The Fourth Amendment and Preflight Searches of Airline Passengers in a Post-9/11 World* (Brigham Young University Law Review, 2006), pp. 1631-1667, at 1657.

238 *United States v. Knights*, 534 U.S. 112, 118-19 (2001) (citing Wyoming v. Houghton, 526 U.S. 295, 300 (1999)).

239 see Title 19 U.S.C. Chapter 4, Subtitle III, Part V, Section 1582 of the Tariff Act of 1930; Title 19 U.S.C. Chapter 3, Subtitle IV, Part 5, Section 482.

240 see *United States v. Ramsey*, 431 U.S. 606, 616 (1977); Vina, Stephen R. *Virtual Strip Searches at Airport: Are Border Searches Seeing Through the Fourth Amendment?* (8 Texas Wesleyan Law Review, 2001-2002), pp. 417-439, at 423.

241 see *Carroll v. United States*, 267 U.S. 132, 154 (1925).

242 *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985).

243 United States v. Niver, 689 F.2d 520 (5th Circuit, 1982).

244 For further discussion, see Vina, Stephen R. *Virtual Strip Searches at Airport: Are Border Searches Seeing Through the Fourth Amendment?* (8 Texas Wesleyan Law Review, 2001-2002), pp. 417-439; Mock, Tobias W. T*he TSA's New X-Ray Vision: The Fourth Amendment Implications of "Body Scan" Searches at Domestic Airport Security Checkpoints* (49 Santa Clara Law Review, 2009), pp. 213-252.

Based on the "border search exception", "[r]outine searches of the persons and effects of entrants are not subject to any requirement of reasonable suspicion, probable cause, or warrant".[245] Non-routine border searches, on the other hand, require reasonable suspicion to be carried out, since they are considerably more intrusive.

A strip search is by law a non-routine (border) search and, thus, requires reasonable suspicion. As the 11th Circuit Court affirms, "[r]easonable suspicion to justify a strip search [at a border] can only be met by a showing of articulable facts which are particularized as to the person and as to the place to be searched".[246] "A strip search under federal law includes the exposure of a person's naked body for the purpose of a visual or physical examination".[247] Alternatively, there are uniform statutory definitions from state legislatures of what constitutes a strip search. As the US Court of Appeals for the 4th Circuit affirmed:

> Virginia's statutory law, which is similar to that of most states, provides that, "[s]trip search shall mean having an arrested person <u>remove or arrange some or all of his clothing</u> so as to permit a visual inspection of the genitals, buttocks, anus, female breasts, or undergarments of such person".[248] (emphasis added).

An X-ray search of an individual's body is also by law a non-routine border search. As the US Court of Appeals for the 11th Circuit affirms:

> In United States v. Pino, 729 F.2d 1357, 1359 (11th Cir.1984), we recognized that the "the amount of [reasonable] suspicion needed for an x-ray [is] ... the same amount needed for a strip search." (citing Vega-Barvo, 729 F.2d at 1345).[249]

---

245 *United States v. Montoya de Hernandez*, 473 U.S. 531, 538 (1985); *United States v. Beras*, 183 F.3d 22 (1st Circuit, 1999).

246 *United States v. Vega-Barvo*, 729 F.2d 1341, 1349 (11th Circuit, 1984).

247 *Amaechi v. West*, 237 F.3d 356 (4th Circuit, 2001).

248 *Ibid.*, citing Va. Code Ann. S 19.2-59.1(F).

249 *Brent v. Ashley*, 247 F.3d 1294 (11th Circuit, 2001).

A patdown is by law a routine border search and thus does not require reasonable suspicion.[250] A patdown, also known as a frisk, is defined as:

> to run the hand rapidly over the outer clothing of (a suspect) for the purpose of finding concealed weapons.[251]

The TSA is a component of the DHS and was established with the enactment of the ATSA, which federalized airport screening. Absorbing the security responsibilities of the FAA, the TSA is now primarily responsible for the security of all forms of public transportation, which includes civil/commercial aviation, and for the development and implementation of security procedures thereof. Under this authority, the TSA is self-regulating the use of body scanners, whereby self-regulations and internal self-reporting, rather than legally binding 'hard' rules and independent, external inspection, are relied upon.

The self-regulations declare that the TSA does not store, print, transmit or export the images produced by the body scanners and the TSA has consistently proclaimed that the machines do not have these capabilities. The TSA also proclaims that it is their policy to use software cloaking or a privacy algorithm, also known as a "modesty filter", which converts backscatter images into what the TSA describes as a "drawing". In addition, a security officer views the images in a remote operator console. However, the rules governing the operating procedures of TSOs using the body scanners have not been revealed, which are supposed to be documented in standard operating procedures (SOPs). The TSA has refused to reveal the rules "due to the sensitivity of the technical and operational details".[252] For the same reason of not wanting to reveal sensitive information of a national security nature, the DHS initially refused to comply with a request under the Freedom of Information Act (FOIA) filed by EPIC for documents, contracts and procedures pertaining to the capabilities and technical specifications of body scanners in use. In response, EPIC filed a FOIA lawsuit against the DHS and, as a consequence, the DHS complied with some of EPIC's demands by disclosing documents that reveal the technical specifications and the procurement contracts for body scanners with Rapiscan and L3.

Contrary to the previous declarations of the TSA that the body scanners are not capable of storing or transmitting the images generated, the documents obtained by

250 see *United States v. Beras*, 183 F.3d 22 (1st Circuit, 1999).

251 Merriam-Webster's Dictionary of Law (1996).

252 Privacy Impact Assessment for TSA Whole Body Imaging, DHS, 17 October 2008, p. 4.

EPIC on TSA operational requirements and procurement specifications instead reveal that the TSA has indeed required that the machines have storage and export capabilities (albeit when in test mode, as opposed to screening mode), and an Ethernet interface connection that supports Transmission Control Protocol/Internet Protocol (TCP/IP).[253] The official documents also confirm that the privacy algorithms can be disabled.

With regards to the admissibility of digital evidence,[254] US courts may apply the Federal Rules of Legal Evidence. Rule 1001 (3) states:

> An "original" of a photograph includes the negative or any print therefrom. If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an "original."

Therefore, an image produced by a body scanner, used to justify the subsequent removal of a passenger's clothes to attain the suspected concealed weapon or contraband, is admissible as evidence in a court of law.

Nevertheless, wrongfully obtained evidence, in violation of the Fourth Amendment, may be excluded from criminal proceedings in a court of law.[255] This is commonly known as the "exclusionary rule." As Rule 402 of the Federal Rules of Legal Evidence states:

> All relevant evidence is admissible, except as otherwise provided by the Constitution of the United States, by Act of Congress, by these rules, or by other rules prescribed by the Supreme Court pursuant to statutory authority. Evidence which is not relevant is not admissible.

In accordance with the E-Government Act of 2002, a Privacy Impact Assessment (PIA) may need to be conducted for body scanners, if indeed the images generated are

---

[253] see Transportation Security Administration, System Engineering Branch, Operational Requirements Document, Whole Body Imager Aviation Applications, July 2006, Version 1.9, Final Report, pp. 10-11; Transportation Security Administration, Office of Security Technology System Planning and Evaluation, Procurement Specification for Whole Body Imager Devices for Checkpoint Operations, 23 September 2008, FINAL, Version 1.02, pp. 4-7.

[254] Digital evidence may include, but is not limited to: the content of computer hard drives, computer printouts, GPS data, e-mails and digital video.

[255] see *Weeks v. United States*, 232 U.S. 383 (1914); Mapp v. Ohio, 367 U.S. 643, 655 (1961).

considered personally identifiable information.[256] A PIA evaluates how personal information in identifiable form is collected, maintained and disseminated by government agencies. PIAs must be conducted before or during the development, procurement or modification of information technology systems, and not after, in order to "ensure sufficient protections for the privacy of personal information".[257] As a result, some argue that PIAs are grounded on the "precautionary principle"[258] and serve as an example of the needed extension of this legal principle to the protection of privacy (Friedewald, M., et al. (eds.): SWAMI Deliverable D3, 2006).[259]

5.9 DEFICIENCIES AND DILEMMAS OF THE US LEGAL FRAMEWORK

After assessing the effectiveness of the US legal framework in protecting privacy, based on the principles of privacy and the criteria of adequacy, significant legal deficiencies and dilemmas in the US come to light, with regards to the use of body scanners.

Even if backscatter body scanners are determined to be the most effective devices for detecting liquid/chemical and plastic explosives, and other threats, which arguably has yet to be decisively proven, numerous privacy concerns and legal questions need to be addressed before this technology is further used on passengers. Fear of an "endless debate" must not overshadow these concerns.[260]

---

256 US Federal courts have held, for example, that a videotape is a "record" for the purposes of the Privacy Act 1974, if the videotape contains the means of identifying the individual concerned (see: *Albright v. United States*, 631 F.2d 915 (D.C. Cir. 1980)). Thus, if the images generated by body scanners are stored in a "system of records", in which the concerned individual's image is identifiable, it is also possible that these images may constitute a "record" for the purposes of the Privacy Act 1974 and are, therefore, in this sense, subject to the Act. However, as argued in the next section, body scanner images may not necessarily constitute information in personally identifiable form.

257 E-Government Act of 2002, Section 208.

258 The precautionary principle was originally developed in the context of environmental protection and refers to the need to anticipate the plausible or potential environmental harm of an act, policy or technology, and to take preventive measures against the potential harm, even if there is uncertain scientific evidence proving the harm is real. The principle is found in the 1992 Rio Declaration on Environment and Development (Principle 15) and is also a core element of the EU's environmental policy.

259 SWAMI (Safeguards in a World of Ambient Intelligence) was an EU project aimed to provide an overview of the key social, legal and ethical implications of ambient intelligence and highlight the privacy threats.

260 Former Homeland Security Secretary Michael Chertoff argued against a potential "endless debate". see Testimony by Secretary Michael Chertoff Before the Homeland Security Subcommittee of the Senate Appropriations Committee, available at: http://www.dhs.gov/xnews/testimony/testimony_0035.shtm

First of all, the legal framework, as it stands, does not fulfill *the* ***use limitation and purpose specification principles***, nor does it ensure *clarity* or *foreseeability*. In terms of regulating the use of backscatter body scanners, the law does not clarify whether the use of backscatter body scanners is a routine or non-routine search or stipulate what level of suspicion is required before their use is permitted and under what legal protections. There is essentially no case law that explicitly defines or clarifies when the use of backscatter body scanners is reasonable and unreasonable or in accordance with the Fourth Amendment.[261]

Since the TSA is already equating the use of (fully-intrusive) body scanners to a routine border search, their use can easily develop into the standard technique or primary means of passenger screening at airports, replacing not only patdowns, but also WTMDs. This was already suggested by (former) TSA Chief Kip Hawley with regards to millimeter wave portals.[262] As Vina points out, "[b]y substituting the Body Scan for a patdown, Customs has ingeniously laid a foundation for a more liberal application of the Body Scan for now and in the future" (2002, p. 436). Hence, the most recent change in TSA's policy regarding the circumstances surrounding the use of active millimeter wave portals.

As a result, eventually no level of suspicion or consent will be required. Once that legal justification is made and their use is considered the norm, there is also nothing to prevent the expansion of the use of body scanners to other locations (and for reasons other than aviation security), particularly if the advancement of body scanner technology increases the speed in which persons can be scanned, decreases the size of the devices, increases their portability, further increases the distance in which people can be scanned from[263] and allows for the incorporation of the backscatter technology within CCTV sur-

---

[261] For further discussion, see Vina, Stephen R. *Virtual Strip Searches at Airport: Are Border Searches Seeing Through the Fourth Amendment?* (8 Texas Wesleyan Law Review, 2001-2002), pp. 417-439; Mock, Tobias W. *The TSA's New X-Ray Vision: The Fourth Amendment Implications of "Body Scan" Searches at Domestic Airport Security Checkpoints* (49 Santa Clara Law Review, 2009), pp. 213-252.

[262] Leib, Jeffrey. "Airport to try tailored security" (The Denver Post, 19 February 2008), available at: http://www.denverpost.com/arcade/ci_8301858

[263] In the Netherlands, the *NRC Handelsblad* reported that it has learned that the Rotterdam police department seeks to develop within three years a portable device that can see through people's clothing to check for concealed weapons. According to *NRC Handelsblad*, Rotterdam's police have received from the government a 500,000-euro grant to develop the device and are now approaching companies, universities and research institutes to develop it. While there are already devices, such as ThruVision's T5000, that can see through people's clothes meters away in the outdoors, portability for the police is also important. see Heck, Wilmer. "Dutch police try to develop x-ray vision" (NRC Handelsblad, 8 January 2010), available at: http://www.nrc.nl/international/Features/article2454112.ece/Dutch_police_try_to_develop_x-ray_vision

veillance cameras.[264] The law's ambiguity could be stretched to initiate the use of body scanners at both public and commercial locations, such as sports arenas, mass transportation areas, government buildings, manufacturing sites, schools or shopping malls.[265]

Nevertheless, a body scan is already currently not genuinely voluntary. Forcing a person to choose between the rights enshrined in the Fourth Amendment and the right to travel "constitutes coercion".[266] As the EU's Article 29 Data Protection Working Party argues, "[m]any passengers will consent to being scanned because by doing so they will avoid potential problems or delays, while their first priority is to get on board of their flight on time. Such consent is not sufficiently free".[267] The Article 29 Working Party further adds that "[i]f the consequences of consenting undermine individuals' freedom of choice, consent would not be free".[268]

In 2008, the US House of Representatives approved H.R. 2200 (Transportation Security Administration Authorization Act), which aims to limit the use of body scanners in airport screening. Contrary to the recent change in TSA's policy on the use of body scanners, Sec. 215 of H.R. 2200 prohibits the use of the devices as the sole or primary method of screening passengers and delineates their use as an optional alternative to patdowns in secondary screening. The bill was referred to the US Senate and, as of January 2012, no further steps have been taken.[269]

While approving specific legislation regulating body scanners is called for, this particular piece of legislation is erroneous. The bill makes no mention of the mandatory use of privacy algorithms and in fact defines a body scanner (termed 'whole body imaging technology') as a device "that creates a visual image of the individual's full body, showing the surface of the skin". The words "showing the surface of the skin" certainly implies that the form of body scanners the bill is referring to include those with their

264 ThruVision's terahertz ray technology already integrates CCTV technology allowing for enhanced public or urban surveillance.

265 For example, the New York Police Department is already testing terahertz imaging scanners (to be placed on police vehicles) for detecting concealed weapons. see Wagstaff, Keith. "Police Developing Tech to Virtually Frisk People from 82 Feet Away" (Time Magazine, 20 January 2012), available at: http://techland.time.com/2012/01/20/police-developing-tech-to-virtually-frisk-people-from-82-feet-away/

266 *United States v. Kroll*, 481 F.2d 884, 886 (8th Circuit, 1973).

267 see Article 29 Data Protection Working Party, WP187, Opinion 15/2011 on the definition of consent, Adopted on 13 July 2011, p. 15.

268 *Ibid*., p. 12.

269 On the other hand, Senators Klobuchar (D-MN) and Bennett (R-UT) introduced a bill that mandates the deployment of body scanners at US airports and mandates their use for primary screening.

full intrusive capabilities intact, i.e. those that generate the graphic images we should be concerned about, rather than those that employ modesty filters or privacy algorithms. Moreover, the bill proposes a framework that equates the use of body scanners, in their full intrusive manner, with appropriately conducted patdowns and permits their use as an alternative to patdowns. Therefore, the proposed bill correctly prohibits the use of fully-intrusive body scanners for primary screening purposes, but incorrectly promotes their use for secondary screening.

To compensate for the fact that a patdown conducted appropriately, or in accordance with the TSA's SOPs, or as described in the TSA's official training manual, is certainly less intrusive than the images generated by body scanners, whether backscatter or millimeter wave, and therefore their use as an alternative to patdowns is not justifiable, the TSA has made patdowns more intrusive. Last year, the TSA announced a new patdown procedure known as the 'enhanced patdown', which included patting down sensitive areas of the body – the breast and groin areas of females and the groin area of males.[270] The enhanced patdown considerably increased complaints from passengers, particularly from female passengers. Since then, the TSA has instructed airport screeners not to touch female passengers between the breasts.[271] Nevertheless, there have been numerous reports that passengers, who refused to go through a body scan and instead opted for a patdown, are being subjected to very thorough patdowns.[272] Moreover, in accordance with the Screening Management SOP, patdowns may still now include the patting of "sensitive areas" of the body if deemed necessary.[273]

On top of that, the law is ***inconsistent*.** Since a X-ray search of an individual's body is considered by law to be a non-routine border search[274] and backscatter body scanners emit X-rays, the minimal or no level of suspicion required at present to use backscatter

---

270 The full body patdown could be similar to the enhanced patdown.

271 see Goo, Sara Kehaulani. "Airport Pat-Down Protocol Changed: Women Complained that Security Checks Were Humiliating" (Washington Post, 23 December 2004), available at: http://www.washingtonpost.com/wp-dyn/articles/A20026-2004Dec22.html

272 Elliott, Christopher. "The Navigator: Some worry that refusing TSA's full-body scan may come at a price" (Washington Post, 2 May 2010), available at: http://www.washingtonpost.com/wp-dyn/content/article/2010/04/28/AR2010042802743.html

273 The Screening Management SOP (Implementation Date: June 30, 2008), which was leaked on the web and is Sensitive Security Information for only the "Need to Know", distinguishes between the different types of patdowns: full body patdowns; bulk-item patdowns; limited patdowns of the stomach area, the back and both legs; and finally patdowns that may include the patting of sensitive areas. The Screening Management SOP is different from the Screening Checkpoint SOP.

274 see *Brent v. Ashley*, 247 F.3d 1294 (11th Circuit, 2001).

body scanners is contrary to case law. Furthermore, given that the end result of backscatter body scanners, without software cloaking, is similar to that of strip searches and far more intrusive than patdowns, the same legal reasoning behind conducting a patdown is inconsistently and wrongfully being applied to the use of backscatter body scanners.

As a result of the legal framework failing to bring clarity and legal foreseeability to the use of body scanners, *the* ***principle of enforcement/redress*** is also not fulfilled. In terms of clarifying when their use by an airport security screener has violated the Fourth Amendment and when evidence has been wrongfully obtained from their use, there are no laws specific enough to be enforceable in a court of law. As the US Supreme Court affirms, "the right allegedly violated must be defined at the appropriate level of specificity before a court can determine if it was clearly established".[275] Similarly, governmental agents are generally "shielded from liability for civil damages insofar as their conduct does not violate clearly established statutory or constitutional rights of which a reasonable person would have known".[276] Consequently, TSA airport screeners or Transportation Security Officers (TSOs) are, at present, arguably shielded from legal action for any inappropriate use of body scanners.

The law, as it stands now, is ***not up to date*** with the capability of the latest visualization technology, since it is not in line with the technological reality that strip searches can occur by electronic means and without the need for a person's clothes to be removed. Furthermore, the law does not permit the ***flexibility*** to adapt to new technologies. Due to the constrained definition of a strip search, generally accepted in the US, the use of body scanners cannot be legally construed to constitute a strip search. Therefore, even if the use of backscatter body scanners poses a similar degree of privacy intrusion as a full body strip search, the law is essentially unable to obligate the same level of suspicion.

The legal framework is ***dependent on self-regulations***. Although the PIA conducted by the DHS on the deployment and use of body scanners essentially approves of the current circumstances surrounding their use, including the self-regulations and operating protocols of the TSA,[277] over relying on the TSA to self-regulate the scope and manner of use of body scanners is naïve at best. Self-regulations, without the corresponding binding 'hard' laws as a basis and without the external enforcement mechanisms in place, are far from reliable. Such an approach to regulation elevates valid

[275] *Wilson v. Layne*, 526 U.S. 603, 615 (1999); reiterating the US Supreme Court's judgment in *Anderson v. Creighton*, 483 U.S. 635, 641 (1987).

[276] *Harlow v. Fitzgerald*, 457 U.S. 800, 818 (1982).

[277] Privacy Impact Assessment for TSA Whole Body Imaging, DHS, 17 October 2008.

concerns of accountability and supervision. But, the TSA already has a history of not always respecting privacy. For instance, the Inspector General of the DHS found that the "TSA did not consistently apply privacy protections in the course of its involvement in airline passenger data transfers",[278] nor reliably disclose to the public the scope of its use and dissemination of passenger data.[279] Besides, the SOPs governing the use of body scanners by TSOs are not ***readily accessible***. Moreover, the PIA conducted on body scanners is fundamentally based, for the most part, on the voluntary use of body scanners for secondary screening and not on the changed policy of the TSA to use body scanners in place of WTMDs for primary screening.

The legal framework pertaining to body scanners is, for the most part, ***ambiguous, altering* and *not legally binding***. Since the self-regulations are not binding or fixed, they could simply change at the discretion of the TSA, regarding, for instance, the employment of a modesty filter or privacy algorithm and the retention of backscatter images. As former TSA Chief Kip Hawley admitted, in an interview with Bruce Schneier, "We [TSA] do not now store [backscatter] images for the test phase (function disabled), and although we haven't officially resolved the issue, I fully understand the privacy argument and don't assume that we will store them if and when they're widely deployed"[280] (emphasis added). The DHS has reportedly asked the manufacturers of backscatter body scanners to de-activate the storage and data export capabilities of body scanners, but the DHS/TSA could just as easily re-activate these capabilities, and no law prohibits the TSA or security screeners from doing so, nor mandates that the body scanner manufacturers must de-activate or completely remove these capabilities in the first place. Essentially, since there is no binding law regulating the manufacture and design of body scanners, there is neither a guarantee that the images will not be stored or transmitted nor a guarantee that a privacy algorithm will always be employed. There is simply no binding law that mandates that the TSA must employ a privacy algorithm. In addition, the self-regulations do not sufficiently restrict the use of backscatter body scanners on children and pregnant women, nor evidently guarantee that an Image Operator or TSO of the same gender of the individual being scanned sees the backscatter images.

The TSA has already drastically altered their policy regarding the circumstances surrounding the use of backscatter body scanners and active millimeter wave portals.

---

[278] Review of the Transportation Security Administration's Role in the Use and Dissemination of Airline Passenger Data (Department of Homeland Security, Office of Inspector General, March 15, 2005), p. 40.

[279] *Ibid*., pp. 42-48.

[280] Bruce Schneier interview with (former) TSA Head Kip Hawley (30 July 2007), available at: http://www.schneier.com/interview-hawley.html

The TSA previously announced that it will begin to pilot active millimeter wave technology in primary screening or in place of WTMDs at six airports (Tulsa International Airport, followed by the International airports in San Francisco, Las Vegas, Miami, Albuquerque, and Salt Lake City). Passengers who refuse to receive millimeter wave screening will undergo *both* walk-through metal detector screening and a patdown.[281] As of November 2009, ten airports are now using the imaging technology for primary screening,[282] and once again the TSA announced plans to use an additional 150 backscatter body scanners in place of WTMDs beginning in 2010. There is thus no guarantee that the use of body scanners, whether the backscatter or millimeter type, will remain as a voluntary alternative to patdowns or WTMDs.

The PIA on body scanners only confirmed that the DHS/TSA indeed intends to entirely replace patdowns for secondary screening with the use of body scanners, and even down the road to replace WTMDs with body scanners for primary screening. As the PIA declares, "[a] subsequent phase will evaluate WBI [Whole Body Imaging] technology for individuals undergoing primary screening".[283] The DHS/TSA is following through with this declaration and is now planning for all passengers to "go through the whole-body imager instead of the walk-through metal detector", as announced by Robin Kane, TSA's Assistant Administrator for Security Technology.[284]

Besides, PIAs, as they stand now, are focused primarily on personal data, and may not be fitting for body scanners. While body scanners generate images of the naked body, the images may not necessarily constitute information in personally identifiable form *per se* or in the legal sense, and nor are personal identifiers or the identification of the individual appended to the images. As a result, since body scanner images may not necessarily constitute a means of identifying the individual concerned, it is unlikely that the Privacy Act 1974 is applicable to the images generated by body scanners. In any case, the Privacy Act 1974 is certainly not applicable when the body scanner images are not actually stored, even though the images produced by (fully-intrusive) body scanners are seriously privacy-invasive.

281 Frank, Thomas. "Body scanners replace metal detectors in tryout at Tulsa airport" (USA Today, 18 February 2009), available at: www.usatoday.com/travel/flights/2009-02-17-detectors_N.htm; "TSA Continues Millimeter Wave Passenger Imaging Technology Pilot", TSA, 18 *February 2009,* available at: http://www.tsa.gov/press/happenings/mwave_continues.shtm

282 see http://www.tsa.gov/approach/tech/imaging_technology.shtm, last visited on 12/11/09.

283 see Privacy Impact Assessment for TSA Whole Body Imaging, DHS, 17 October 2008, p. 2.

284 Sharkey, Joe. "Whole-Body Scans Pass First Airport Tests" (New York Times, 6 April 2009, available at: http://www.nytimes.com/2009/04/07/business/07road.html?_r=1

The legal framework pertaining to privacy was equally designed to control data as traditionally understood and not to regulate privacy intrusion in other domains, such as the human body (Wood, 2006, p 89). The Privacy Act 1974, for instance, regulates how government agencies may collection, use, disseminate and retain personally identifiable information, and therefore it is immediately questionable if the nearly 40-year-old piece of legislation can effectively regulate body scanners. Moreover, the set of Fair Information Practice Principles (FIPPs), developed by the DHS, and used by the TSA as a template in the PIA on body scanners, oddly omit the essential principles of enforcement/redress and proportionality.

In addition, the legal framework, as it stands, does not fulfill the ***principle of proportionality***. The law does not do enough to prevent the prospective required use of body scanners in their full intrusive capability on all air travelers, which would force hundreds of millions of people to be subjected to a strip search by electronic means. This would undoubtedly cause the potential use of body scanners to be disproportionate and unreasonable, since certainly that many people do not pose a threat to aviation security nor exhibit a reasonable level of suspicion to justify being electronically or digitally strip-searched.

Already the current approach of using body scanners is not proportional to their purported aim of ensuring the security of commercial aviation. If a traveler, whether domestic or international, sets off a walk-through metal detector at an airport's security checkpoint or 'arouses' a minimal level of suspicion or is randomly selected for additional or secondary screening, known as "sweep screening," or is selected by the Computer Assisted Passenger Profiling System (CAPPS), he or she is normally subject to a patdown or other special screening requirements. Even passengers wearing loose-fitting clothes, for instance, could be selected for secondary screening for unduly suspicion that they could be hiding something. Since TSA airport screeners, as a matter of policy, are currently using body scanners, where deployed, as an alternative to patdowns, their use automatically in practice does not require the same level of suspicion, if any, as a strip search. According to the TSA, an estimated two million passengers per week or 15% of air travelers are selected for patdowns.[285] As a result, millions of passengers, who do not pose a threat to the security of commercial aviation, may potentially be subjected to a strip search by electronic means in order to exercise their right to travel.

The "reasonable expectation" of privacy, which is the foundation from which privacy is defined in the US, is also problematic. As a number of legal scholars have argued, the *Katz* test is flawed in that unless an individual takes extraordinary steps or

[285] see Kehaulani Goo, Sara. "TSA Keeping Pat-Down Procedures in Place," (4 December 2004), available at: http://www.washingtonpost.com/wp-dyn/articles/A33790-2004Dec3.html

affirmative measures to protect his or her privacy, he or she does not have a subjective or reasonable expectation of privacy (Kearns, 1998, p. 1005; Paton-Simpson, 2000, p. 306). In addition, as Minert points out, society's expectation of privacy could easily become a mere echo of the government's expectation of privacy (2006, pp. 1653-54). Similarly, as the *Report on the Surveillance Society* argues, the reasonable expectation of privacy will surely be depressed if people "get used to" increasingly more surveillance (Wood, 2006, p. 80). This argument is consistent with the US Supreme Court's judgment in *Kyllo v. United States* that the more widespread the deployment and adoption of a particular technology the less "reasonable expectation" of privacy the public enjoys with respect to its use.[286] This is also somewhat true for body scanners, as their deployment becomes increasingly widespread and well-known publicly. Moreover, the never-ending advancement and escalating deployment/use of PITs gradually diminishes our "reasonable expectation" of privacy, as people view the outcome to be increasingly necessary for their security/safety.

Although there is some case law applicable to backscatter body scanners, as outlined above, there is nevertheless a vacuum of law, which courts are left to fill in. Essentially, US statutory laws are inadequate for regulating the use and manufacture of backscatter body scanners. As a result, the legal framework is ***primarily dependent on case law*** for direction.

In sum, the US legal framework is inadequate to safeguard privacy with regards to the deployment and use of body scanners. Under the current conditions, whereby the employment of a privacy algorithm or the deletion of the images is not mechanically or automatically guaranteed and other safeguards are not legally binding, the use of body scanners as a primary means or secondary means of passenger screening is disproportionate and constitutes an unjustified violation of privacy in a democratic society. With the growing use of body scanners at airports across the US, the law, as it stands now, is unable to adequately uphold the integrity of the Fourth Amendment or defend the right to bodily privacy.

[286] see *Kyllo v. United States*, 533 U.S. 27, 34 (2001).

5.10 RECOMMENDATIONS ON ENHANCING THE US LEGAL FRAMEWORK

If we adopt the "originalist" or "textualist" approach to understanding the US Constitution,[287] then entirely new laws should be adopted, when deemed necessary, by elected legislators/representatives, instead of over relying on the interpretations of judges, which can sometimes vary or be inconsistent.

Even if the use body scanners are deemed proportional to the legitimate aim of diminishing the threat posed by plastic guns, ceramic knives, and liquid, chemical, plastic explosives, new and specific laws are necessary nonetheless. Any new and specific legislative act on body scanners must be based, in part, on the principles of privacy, since body scanners and their growing deployment and use at airports are a threat to the right to privacy and the constitutional protections of the Fourth Amendment. Specific laws for body scanners, enacted by the US Congress, would eliminate the excessive dependence on US courts to fill in the existing legal vacuum. After all, only the legislative branch is meant to create law in the US, as opposed to the judicial branch, which is principally meant to apply it.

Legislation can either primarily regulate the design and manufacture of backscatter body scanners (rules on technical specifications) or instead primarily regulate their use (rules on operating standards). In other words, the full intrusive capabilities of body scanners can be maintained, while their use is strictly regulated, or the intrusive capabilities can be permanently limited during design and manufacture, thereby not requiring such strict regulation on their use. Either way, legislation should apply, where applicable, the core principles of privacy.

Focus on manufacturer-level regulations/laws

Regulation at the manufacturer-level should permanently minimize the intrusion upon privacy from the get-go. The burden is placed considerably more on the manufacturers rather than on the airport screeners. Legislation should mandate the automatic, built-in employment of a privacy software algorithm, in order to greatly reduce the intrusiveness of (backscatter) body scanners, thereby minimizing the infliction of indignity and humiliation upon individuals. It is important to note that the meaning of "built-in" here refers to the permanent employment of the software solutions, rather than a software add-on approach. The software can blur out the face and genitals and/

[287] This approach is, for example, prominently advocated by US Supreme Court Justice Antonin Scalia. see, e.g., Scalia, Antonin. *A Matter of Interpretation: Federal Courts and the Law* (Princeton University Press, 1997).

or obscure the details associated with the entire body, in what is known as a "virtual fig leaf" or "modesty filter". These capabilities are already available and are increasingly being further developed. Rapiscan, for instance, developed software that converts body scanner images into "generic figures", which resemble an *avatar*, as opposed to an image of an individual's genitals.[288] However, it is essential to ensure that the effectiveness of these privacy algorithms or software solutions are validated and cannot be circumvented.[289] Moreover, in no circumstances, should the privacy algorithms or filters or software solutions be capable of being disabled at airports.

Nevertheless, the creation of a "drawing" or "chalk outline" of one's body, as it is often described as or referred to, may still remain somewhat or slightly intrusive and therefore, based on the ***use limitation and purpose specification principles,*** built-in restrictions on the ability to print, retain or otherwise distribute/export the backscatter images must be ensured. However, in exceptional circumstances, when a weapon or contraband is revealed, the limited retention, export or printing may be necessary as evidence in a court of law to justify the subsequent (targeted) patdown or, if legitimately justified, an ordinary strip search if challenged by the defendant. This may also be helpful to satisfy the ***access/participation principle***. On the other hand, the retention of body scanner images may not be required at all. Nevertheless, in these very exceptional circumstances, if indeed required, an additional secure password, entered only by the Supervisory Transportation Security Officer (STSO), could override the built-in restriction and enable the image to be retained. This event must be automatically recorded.

In order to ensure the image data transmitted between the backscatter body scanners at the security checkpoint and the remote operator consoles is not intercepted, based on the ***security principle***, the images must be encrypted and on top of that transmitted via a secure cable connection. The manufacturer must equally be required to ensure that the software fixes and built-in restrictions cannot be easily undone or bypassed.

Perhaps, in order to undeniably diminish the intrusive capability of body scanners, the images generated can also be monitored, like in Brijot's imaging system, by an intelligent detection engine. However, intelligent detection software (also known as automatic threat recognition or ATR) may still require further advancement and testing in

[288] The software upgrade may be tested by the TSA. See Hughes, John. "Airport 'Naked Image' Scanners May Get Privacy Upgrades" (Bloomberg, 8 September 2010), available at: http://www.bloomberg.com/news/2010-09-08/airport-naked-image-scanners-in-u-s-may-get-avatars-to-increase-privacy.html

[289] Marc Rotenberg, Executive Director of EPIC, made this point during a brief discussion at the third annual international conference *Computers, Privacy and Data Protection* (29-30 January 2010, Brussels).

order to be a trustworthy replacement of well-trained screeners.[290] Indeed, the development and testing is occurring. Software, developed by L-3, capable of analyzing body scanner images for threats, locating those threats and raising an alarm, could replace the need for human operators to view the images altogether. The software is currently being tested at Amsterdam's Schiphol Airport and the initial results are reportedly positive.[291] In addition to removing the need for a remote operator or viewer, the ATR capabilities can also potentially reduce the security implications of human errors. With ATR capabilities, security checkpoint personnel will only need to resolve the alarms by conducting, for instance, a targeted patdown of the area on a person where the (potential) threat (metallic or non-metallic object) was detected. The TSA is also evaluating the viability and effectiveness of the ATR capabilities, with ongoing trials, and a successful certification process is expected.[292]

Essentially, once the intrusive capabilities of backscatter body scanners are without a doubt considerably and permanently narrowed, as guaranteed by the various technological limitations, including validated and trustworthy privacy algorithm/software solutions, their use will not qualify as a *strip search by other means* and will be less intrusive than a patdown. Therefore, strictly under these conditions, body scanners may qualify as a routine search and may constitutionally replace (full body) patdowns as a mandatory means of secondary screening at airports and even perhaps legitimately replace the use of WTMDs altogether for primary screening, which does not require reasonable suspicion. This is contrary to Mock's (2009) view that backscatter body scanners may not replace WTMDs, since a "drawing" or "chalk outline" of one's body is more intrusive than a magnetometer search (Mock, 2009, p. 238).

Evidently, body scanners, even with the employment of a privacy algorithm, are considerably more effective than WTMDs, patdowns and other alternative devices in

---

290 As pointed out by *Eckard Seebohm*, Head of the Aviation Security Unit of the European Commission during the first Body Scanners Task Force public consultation meeting held on 12 December 2008 at the Centre Albert Borschette in Brussels.

291 During the second meeting (which I also attended) of the Task Force on Security Scanners, established by the European Commission, representatives from the Netherlands (the National Coordinator for Counterterrorism –NCTb) explained the success of the ATR software. The representatives also noted that the Data Protection Authority in the Netherlands has referred to the body scanners currently in use at Schiphol Airport as a "perfect example" of *privacy by design*.

292 see Tessler, Joelle and Arthur Max. "Better airport scanners delayed by privacy fears" (Associated Press, 28 December 2009); Hughes, John. "Airport 'Naked Image' Scanners May Get Privacy Upgrades" (Bloomberg, 8 September 2010), available at: http://www.bloomberg.com/news/2010-09-08/airport-naked-image-scanners-in-u-s-may-get-avatars-to-increase-privacy.html

helping to detect a variety of potential threats to aviation security. The mandatory use of modestly intrusive body scanners for secondary screening should satisfy those who argue that consent or offering a choice will cancel the security benefits of body scanners. This is a valid point, since terrorists will more than likely choose an ordinary patdown over being body scanned, as there is a far greater chance of finding a hidden threat with body scanners, especially if that threat is a relatively small amount of chemical or plastic explosive hidden very near to his or her genitals. The mandatory use of minimally intrusive body scanners for primary screening on all passengers should satisfy those who warn of the terrifying insufficiency of WTMDs and should eliminate the concerns over the discriminatory manner in which body scanners may be used. While minimally intrusive body scanners are more intrusive than WTMDs, here the significant security gains are arguably proportional to the somewhat greater privacy intrusion.

Nonetheless, proponents of body scanners argue that privacy algorithms could compromise the security benefits of the devices. A virtual fig leaf, for instance, could prevent a backscatter body scanner from revealing a plastic explosive attached to or near an individual's genitals. The immense intrusive capability of backscatter body scanners and the full-body graphic images they generate is indeed what makes them very effective security devices. If, however, the images generated by body scanners remain fully intrusive, then the law must strictly regulate their use to ensure it is proportional to the security gains and that the right to privacy and freedom from unreasonable search and seizure is preserved.

Focus on user-level regulations/laws

Regulating the use, legislation should essentially harden the policies and self-regulations of the TSA, guaranteeing that they remain unchanged and are legally binding.

In addition to built-in restrictions on storing, printing and transmitting the images produced by body scanners, in line with the ***use limitation and purpose specification principles***, the TSOs who view the images (Image Operators) should in no way be able to see simultaneously in person the passengers while being scanned. This can be accomplished through the continued use of remote operator/viewer consoles. The passenger being scanned should also remain unidentified, except in circumstances when a weapon or contraband is revealed. The law should also explicitly mandate that an Image Operator of the same gender must inspect the images, unless under extraordinary circumstances, which may occur where a TSO of the same gender is not available due to staff shortages or emergencies, in accordance with the Screening Management SOP with regards to patdowns.[293] Moreover, to better ensure the images do not exist anymore than is needed for the purpose for which they were created and are not publicly disclosed in any way, cameras and mobile phones must also be absolutely forbidden within a remote operator console. This will prevent airport security personnel from taking photographs of the computer screens that display the images. Accordingly, based on the ***use limitation principle***, the law must prohibit any (unlawful) storage, photograph or public disclosure of the images.

Furthermore, in accordance with child pornography laws, the use of body scanners, at their full intrusive capability, on children and pregnant women must be restricted. The law must therefore specifically mandate that the images of children must always, without exception, employ software cloaking. The creation of body scanner images of children without software cloaking should be explicitly criminalized.

A "trusted passenger program"[294] could be implemented, whereby qualified frequent flyers, which have volunteered sensitive data and have gone through an extensive security assessment/background check, are exempted from body scanners, unless they also arouse a reasonable level of suspicion. The TSA has already rolled out a similar program, known as "Precheck", whereby approved travelers go through WTMDs instead of body scanners.

Based on the ***enforcement principle***, a dedicated screening supervisor at each airport or the corresponding STSO, under the management of the Transportation Security Manager (TSM), should conduct the direct supervision of the compliance of these binding rules (rather than simply general uniformed personnel of the TSA or TSOs). Thus, the responsible individual should have the power to initiate the dismissal of any airport screener who repeatedly fails to comply. In addition, a dedicated oversight committee, together with the DHS Office of Civil Rights and Liberties, DHS Privacy Office, and the Privacy & Civil Liberties Oversight Board,[295] could direct the nationwide compliance of the rules.

In addition to the capacity of air travelers to bring a claim against the US Government (or private security screeners that act on behalf of the government, for the unreasonable or unlawful use of body scanners), the DHS Traveler Redress Inquiry

---

[293] see the Screening Management SOP (Implementation Date: June 30, 2008).

[294] see Aviation and Transportation Security Act of 2001 (Public Law 107-71), SEC. 109.

[295] The Privacy and Civil Liberties Oversight Board (PCLOB) was established after recommended by the National Commission on Terrorist Attacks Upon the United States (known as the 9/11 Commission). The PCLOB is as an independent agency within the executive branch.

Program (DHS TRIP)[296] or a dedicated redress program, in accordance with the ***redress principle***, must facilitate an immediate investigation of such claims. While the Privacy Act 1974 limits judicial remedy, under the legislative act, to US citizens or US lawful permanent residents (LPRs), significant to the use of body scanners at airports, TRIP is open to all individuals regardless of whether they are US citizens, LPRs or simply visitors to the US. Therefore, as a matter of DHS policy, foreign passengers or non-US persons could also have the right to seek (administrative) redress for the wrongful use of body scanners. However, preferably the law should open the door for foreign passengers or non-US persons to seek judicial remedy for the unlawful, disproportional or inappropriate use of body scanners.[297]

Based on the ***principle of proportionality***, the use of backscatter body scanners, <u>at their full intrusive capability</u>, must require the same level of reasonable suspicion as a strip search and must not be equated with an appropriately conducted patdown. In order to do so, the definition of a strip search must be modified to equate the use of backscatter body scanners and other similarly intrusive technology to a virtual strip search, thereby causing their use to be considered a non-routine search. For clarity, the content of the definition would need to accommodate for the fact that a strip search is possible by electronic means and without the need for a person's clothes to be removed. A definition of a strip search, in line with backscatter technology, and anticipatory of the further advancement of similarly intrusive technology, such as <u>active</u> millimeter wave portals, should read as follows:

> *A strip search shall mean the visual inspection of the genitals, buttocks, anus, female breasts, or undergarments of an individual either in person or through <u>any</u> electronic means.*

Above and beyond the laws that regulate the manufacture and/or use of body scanners, the airports that have opted out of federal screening and switched to qualified, authorized private airport security screening companies, in accordance with the Aviation and Transportation Security Act of 2001,[298] should perhaps have the freedom to decide

---

[296] DHS TRIP serves as a means for individuals who believe they have been improperly denied entry or identified for additional screening by a DHS component at a transportation hub to file a request for redress.

[297] The legal fact that the Privacy Act of 1974 limits judicial remedy to US citizens or US legal permanent residents has been criticized by the EU in the negotiations with the US over a transatlantic binding agreement on the exchange of data for law enforcement purposes and the protection of privacy thereof. see the Final Report by EU-US High Level Contact Group on information sharing and privacy and personal data protection, May 2008.

[298] Aviation and Transportation Security Act of 2001 (Public Law 107-71), SEC. 108.

whether or not they want to deploy body scanners in the first place. However, the decision to permit this option is certainly debatable.

The deployment of *minimally intrusive* body scanners at other locations (e.g. train stations or major sports stadiums) may also be permissible on a case-by-case basis. Nevertheless, even if privacy algorithms and other technical measures are permanently employed to safeguard privacy, the law must also prohibit the deployment and use of body scanners by private actors (other than authorized, private airport screening companies).

Lastly, in order to improve security overall, similar to the California Penal Code,[299] Federal law should prohibit the commercial manufacture of knives undetectable to WTMDs by mandating that all knives contain a minimum quantity of metal.

5.11 MANUFACTURER-LEVEL OR USER-LEVEL REGULATION?

Whether manufacturer-level or user-level laws/regulations for regulating body scanners should be predominantly chosen depends on which is a better approach or policy option for balancing privacy with security.

The automatic, permanent incorporation of privacy filters or algorithms, within the images generated by body scanners, can implement the privacy principles and, in doing so, can lawfully and justifiably increase both the deployment and employment of body scanners at airports. Therefore, the manufacturer-level approach can, at the same time, both increase security gains and protect the privacy of a person's body by reducing the level of graphic detail contained in the images. In addition, privacy algorithms do not necessarily cancel the security gains of body scanners, but rather can potentially help airport screeners, albeit with some further training and technical advancement, to objectively detect threatening objects. The potential for developing effective intelligent detection software can further aid in this detection. Any questionable identification of objects to the airport screener could perhaps be compared with the images of known objects before a decision is made to proceed with a patdown.

Since the user-level regulatory approach will maintain the full graphic details of the images generated by body scanners, their use will only constitutionally replace strip searches, and therefore will neither address the flaws of the primary nor secondary means of security screening.

In the long run, therefore, the manufacturer-level regulatory approach may favor both privacy and security, but nonetheless manufacturer-level regulations/laws will

[299] see Section 12001.1 of the California Penal Code.

need to be combined with some user-level regulations/laws, in order to ensure the fulfillment of all the principles of privacy.

5.12 INTERNATIONAL DEPLOYMENT, DEVELOPMENTS AND RESPONSES

The deployment of backscatter body scanners and active millimeter wave portals is gradually spreading around the world. In Europe, the Netherlands and the UK are leading the way in testing and deploying body scanners. In Italy, the Italian Civil Aviation Authority has also deployed and tested body scanners in Rome and Milan and, in Rome's second largest airport, Brijot's passive millimeter wave imaging technology was also tested. Body scanners were also tested in France and Germany.

The UK began testing active millimeter wave portals in 2006 at London's Heathrow Airport and Paddington Railway Station, and began testing backscatter body scanners at Manchester's international airport. Body scanners are being deployed in more airports across the UK. Previously, there were even proposals to install millimeter wave portals throughout London's tube stations,[300] but this was later rejected due to impracticalities.[301] Instead of offered as an alternative to patdowns, passengers in the UK are randomly chosen. There are also calls and initiatives for the compulsory use of body scanners in all UK airports. Concerns previously emerged that the body scans deployed in the UK allow the images to be printed, after it was reported that body scanner images of the 'Bollywood' movie star Shah Rukh Khan were distributed among London's Heathrow Airport security personnel.[302]

On the other hand, Her Majesty's Revenue and Customs (HMRC), a UK governmental department responsible for administering screening measures at points of entry and exit, had also previously took a step in the right direction for privacy and awarded a contract to Brijot Imaging Systems Inc. for its privacy-friendly BIS-WDS® GEN 2 millimeter wave systems, which will be deployed at airports.[303]

300 Webster, Ben. "Body scan machines to be used on Tube passengers" (Times Online, 8 July 2005), available at: http://technology.timesonline.co.uk/tol/news/tech_and_web/personal_tech/article541746.ece

301 "Tube to reject passenger scanners" (Kable, 16 March 2006), available at: http://www.kablenet.com/kd.nsf/Frontpage/85C58F53F411521180257132005EF49F?OpenDocument

302 Shah Rukh signs off sexy body-scan printouts at Heathrow (Yahoo India News, 6 February 2010), available at: http://in.news.yahoo.com/43/20100206/908/ten-shah-rukh-signs-off-sexy-body-scan-p.html

303 Brijot, Press Release (14 December 2007), available at: http://www.brijot.com/assets/pdf/pressreleases/HMRC%20PR%20Web.pdf

In the Netherlands, active millimeter wave portals were deployed in 2007 at Schiphol International Airport. However, rather than initially being used on a trial basis, they have already been formally introduced into the screening process at several security checkpoints. As a joint initiative of the National Coordinator for Counterterrorism (NCTb), Customs authorities and Schiphol Airport, the use of millimeter wave portals, like in the US, is self-regulated. However, these self-regulations are backed by comprehensive privacy/data protection legislation in the Netherlands. According to the self-regulations, the image analyst sits in a closed space and cannot see in person the passenger who is being scanned and the images are not saved. Rather than using a modesty filter, only the face of the passenger is made "unrecognizable" in the images.[304] Although the millimeter wave portals are voluntary, meaning that passengers have a choice between millimeter wave portals or going through regular security procedures, this is only for the time being[305] and, like the self-regulations of the TSA, is subject to change. Already, Schiphol Airport is planning to deploy more body scanners and all passengers flying to the US must go through body scanners since the so-called "Christmas Day attack".

The EU was en route to adopting body scanners as a common method of passenger screening, but that was previously put on hold. Article 4(2) of Regulation (EC) No 300/2008 on common rules in the field of civil aviation security requires the European Commission (EC) to adopt general measures on aviation security, which must include the 'methods of screening allowed'. The EC then proposed in a draft regulation the use of body scanners as a means of screening passengers at airports. In response, the European Parliament voted overwhelmingly to demand a full study on the impact of body scanners relating to fundamental rights, privacy and health before taking a decision on the introduction of body scanners at airports, noting that the use of body scanners is "equivalent to a virtual strip search" and has "a serious impact on the fundamental rights of citizens".[306]

As a result, the EC, and more specifically the Body Scanners Task Force, prepared a communication,[307] in consultation with the Article 29 Working Party, EDPS and other interested parties and stakeholders, and based on the answers received to a questionnaire

[304] Schiphol International Airport, available at: http://www.schiphol.nl/media/portal/_news/pdf/pdf_files/flyersecurityscan_v1_m56577569830813442.pdf

[305] Schiphol International Airport, available at: http://www.schiphol.nl/

[306] European Parliament resolution of 23 October 2008 on the impact of aviation security measures and body scanners on human rights, privacy, personal dignity and data protection.

[307] Communication from the Commission to the European Parliament and the Council on the Use of Security Scanners at EU airports (COM (2010) 311 final), 15 June 2010.

made available to the public.[308] The communication addresses the European Parliament's concerns and questions and briefly provides an assessment on the effectiveness of body scanners on enhancing aviation security. Meanwhile, as a consequence of the so-called "Christmas Day attack", the US upped the pressure on Europe to deploy body scanners.[309] But, the EU remained steadfast on its previous commitment to wait until the EC completes their assessment of the privacy concerns and validated security benefits of body scanners before deciding on whether or not to bring forward legislation on a common EU approach to deploying and using body scanners as a method of screening at EU airports and under what conditions. During the second meeting of the Task Force on Security Scanners, the EC announced that an *impact assessment* on body scanners will be launched and completed next year (2011).[310] The EC urged that a common EU approach

[308] The first meeting/public consultation of the Task Force on Security Scanners was held on 12 December 2008 at the Centre Albert Borschette in Brussels, of which I was an active participant. The meeting was chaired by *Eckard Seebohm*, Head of the Aviation Security Unit of the European Commission. Present at the meeting were numerous relevant stakeholders, including representatives of the manufactures of the different body scanners on the market (L3, Brijot, Rapiscan, Millivision and others), the International Air Transportation Association (IATA), ACI Europe, Schiphol Airport, the Dutch Ministry of Justice, the CEBRN programme of the UK Home Office, the Article 29 Working Party, European Data Protection Supervisor (EDPS), Fundamental Rights Agency (FRA), the European Cockpit Association (ECA), and the assistant to MEP Philip Bradbourn, an outspoken critic of body scanners. There was essentially a consensus among the stakeholders that body scanners are significant for enhancing aviation security, but certain privacy safeguards are required. Indeed, the EDPS and FRA are not completely against body scanners, but are instead hesitant. I pointed out the need to incorporate 'privacy by design' solutions, which representatives from the Article 29 Working Party, FRA and EDPS equally advocated. Representatives of L3 and Rapiscan confirmed that design solutions are feasible and already available and may include anything from blurring the face to converting the body scanner images into animations or even holograms. The representative from L3 further expressed the concern that manufacturers of body scanners have not been given any clear standards to follow during the design and development of the body scanners. I raised the notion that passive millimeter wave imaging is a privacy-friendly alternative to backscatter body scanners or active millimeter wave portals, which of course delighted the representative of Brijot. However, the representatives from Schiphol Airport objected to this point and noted that Brijot's systems do not provide images that are clear or detailed enough to offer the same degree of security benefits of active millimeter wave portals or backscatter body scanners.
In a follow-up email to a Policy Officer at the Aviation Security Unit, nearly a year after the task force meeting and closing of the public consultation, I learned on 26/11/09 that no summary for that consultation was published, no further meeting was scheduled and a legal initiative was yet to be foreseen. In other words, the EC was taking their time to develop the report/communication requested by the European Parliament. However, as a consequence of the "Christmas day attack", the EC accelerated the adoption of this communication on body scanners, which was published in June 2010.

[309] see Hsu, Spencer S. "U.S. to push foreign governments to use body scanners at airports" (Washington Post, 8 January 2010), available at: http://www.washingtonpost.com/wp-dyn/content/article/2010/01/07/AR2010010704282.html

[310] Upon invitation, I also attended the second meeting of the Task Force on Security Scanners, held 14 September 2010 in Brussels. The meeting served to further debate some of the key privacy and health issues/impacts surrounding body scanners, and to discuss the detection performance of body scanners. In addition to representatives from various stakeholders, representatives from EU Member States were also present at the meeting.

be taken, in order to better ensure both the protection of privacy and other fundamental rights and the maintenance of aviation security. The EC also urged that a combination of technical specifications and operational rules is the way forward.[311]

In 2011, the European Parliament approved the deployment of body scanners at EU airports, but banned the use of the backscatter type and insisted that passengers continue to have the right to refuse to be scanned. Although the EU has in the end approved of the use of body scanners, at least there is an apparent agreement within the EC and among most EU Member States that specific, fixed and binding legislation should regulate the development, deployment and use of body scanners throughout the EU, unlike in the US where there is still an excessive reliance on altering self-regulations. Since air passengers travel from the US to the EU and vice-versa, they arguably deserve the same level of privacy protection. For that reason, US and EU regulations on body scanners should be similar. On the other hand, if the EU does not adopt a common position on the deployment and use of body scanners, then it will be up to EU Member States to adopt their own regulations.

Body scanners were also tested at Melbourne International Airport in Australia, which at the time decided not to blur out the genitals in the images,[312] and the Australian Government announced its decision to deploy body scanners at airports throughout the continent.

According to a survey study conducted by the IT firm Unisys in April 2010, as part of the Unisys Security Index, the vast majority of air travelers in the UK, Germany, Netherlands and Australia, with the exception of Spain, are apparently willing to support, to a certain degree, the deployment and use of body scanners, in return for greater aviation security.[313]

The US has also been pressuring additional countries to deploy body scanners and urged the International Civil Aviation Organization (ICAO) to adopt an agreement on improving security standards with the help of body scanners. Whether or not the deployment of body scanners will be globally accepted is yet to be seen.

---

[311] Communication from the Commission to the European Parliament and the Council on the Use of Security Scanners at EU airports (COM (2010) 311 final), 15 June 2010.

[312] see Shears, Richard. "Airport admits 'strip search' body scanners WILL show people naked," (Daily Mail, 15 October 2008), available at: http://www.dailymail.co.uk/news/article-1077800/Airport-admits-strip-search-body-scanners-WILL-people-naked.html

[313] The survey results are available at: http://www.unisyssecurityindex.com/

5.13 CONCLUDING REMARKS

Although the legal framework in the US does not require a complete overhaul, in order to ensure that the deployment and use of body scanners is both constitutional and proportional and does not erode the right to (bodily) privacy, specific statutory laws are required.

The use of body scanners potentially offers immense security benefits and should certainly not be outright prohibited. However, until the necessary binding laws are adopted and put into effect concerning their manufacture, use and deployment, the violation of privacy is disproportionate. In the meantime, there are alternative means of ensuring the security of commercial aviation, albeit probably not as effectively, which can also ensure privacy and uphold the integrity of the Fourth Amendment.

6 PUBLIC SPACE CCTV MICROPHONES and LOUDSPEAKERS: The ears & mouth of 'Big Brother'

6.1 CHAPTER INTRODUCTION

With the exception to where there is an overlap with visual surveillance in public spaces, this chapter specifically addresses the concerns of the public space audio surveillance capabilities of integrated CCTV microphones and the added threat to privacy and liberty posed by the integration of public CCTV loudspeakers.

Section 6.2 introduces the privacy-intrusive evolution of CCTV surveillance technology. Section 6.3 outlines the social and privacy implications of the CCTV microphones and loudspeakers, and how CCTV microphones and loudspeakers are changing the nature and long-established notion of the public space. Section 6.4 reveals the scope of deployment of CCTV microphones and loudspeakers in the UK, whether privately or publicly owned and operated. Section 6.5 outlines the problems, weaknesses and deficiencies of earlier CCTV systems and explains the potential security gains of attaching microphones and loudspeakers to CCTV cameras. Section 6.6 describes the potential alternatives to CCTV microphones and loudspeakers. Section 6.7 gives an overview of the statutory laws and case law of special relevance in the UK. Section 6.8 evaluates and highlights the relevant deficiencies and dilemmas of the UK legal framework in terms of safeguarding privacy and individual liberty with regards to the deployment and use of CCTV microphones and loudspeakers. Section 6.9 proposes relevant policy and legislative recommendations to enhance the UK legal framework. Section 6.10 concludes with a brief summary and some ending remarks.

6.2 THE (PRIVACY-INTRUSIVE) EVOLUTION OF CCTV SURVEILLANCE TECHNOLOGY

CCTV ('Closed-Circuit Television') cameras have been in existence for decades, but during the turn of the 20th Century, particularly in the UK, the number of CCTV cameras deployed has increased dramatically. There are millions of CCTV cameras in the

UK alone.[314] As a result, CCTV cameras continue to play a visually prominent role in the "surveillance society" the UK is rapidly entering.

The ongoing evolution of CCTV technology has evolved from expensive, fixed cameras connected to videocassette recorders (or VCRs) via cables, which recorded and stored restricted amounts of low-resolution video data, to affordable IP (Internet Protocol) addressable, wireless pan/tilt/zoom (PTZ) CCTV cameras, which can be both remotely accessed and controlled, and can record practically unlimited amounts of digital, high-resolution video data, transmitted to computer hard drives for storage and analysis. If a dedicated communications network is not available, the digital video data recorded from these next generation public surveillance cameras can also now be transmitted and easily made available over the Internet or even via mobile phone technologies (Cannataci, 2010).

Other ongoing and/or potential enhancements to public surveillance cameras include the integration of: automatic license plate recognition systems that can track drivers; biometric technology (e.g. advanced face-recognition technology) that can be used to rapidly identify individuals; intelligent software that can recognize in real-time unlawful behavior, activities or events and certain objects;[315] microphones (or audio sensors) that can record audio data; loudspeakers that can enable CCTV control room operators to communicate with people; RFID readers that can track people in possession of RFID tags; software agents that can automatically and purposefully mine the vast

---

314 "FactCheck: how many CCTV cameras?", Channel 4 News,18 June 2008, available at: http://www.channel4.com/news/articles/society/factcheck+how+many+cctv+cameras/2291167

315 The Intelligent Video Surveillance (IVS) market is growing rapidly. Honeywell's Active Alert® and Keeneo's tailor-made software are just two examples of systems on the market that can automatically determine and classify different human behaviours and alert CCTV operators. Portsmouth has recently become the first city in the UK to set up a network of 'intelligent' cameras that can alert CCTV operators of 'suspicious' behaviour. see Slack, James. "Minority Report comes to Britain: The CCTV that spots crimes BEFORE they happen" (Daily Mail, 28 November 2008), available at: http://www.dailymail.co.uk/sciencetech/article-1089966/Minority-Report-comes-Britain-The-CCTV-spots-crimes-BEFORE-happen.html; '"Sci-Fi Film' CCTV Predicts Crime" (Sky News, 27 November 2008), available at: http://uk.news.yahoo.com/5/20081127/tuk-sci-fi-film-cctv-predicts-crime-45dbed5.html; An 'intelligent' CCTV camera, nicknamed "the Bug", designed to predict when a person may be about to commit a crime, is also being tested in high streets and shopping centers in the UK. The camera consists of a ring of eight cameras scanning in all directions. Software linked to the camera can determine when anybody is behaving unusually or suspiciously. A ninth camera then zooms in to follow that person. see Iredale, Will and Chris Gourlay. "CCTV camera 'tails' suspects" (Sunday Times, 15 April 2007), available at: http://www.timesonline.co.uk/tol/news/uk/crime/article1655200.ece; There are also a number of ongoing projects funded by the EU to improve the functionality and reliability of IVS. For example, Project SAMURAI and Project ADABTS aim to develop intelligent public surveillance software integrated with CCTV cameras for real-time behaviour profiling. Project Smart-Eyes (SEARISE) is even more advanced. The project's consortium aims to develop an "artificial cognitive visual system" for detecting, tracking and categorizing salient events and behaviours. The plan is to test the system in large crowded public spaces, once completed in 2011.

amounts of visual and audio data generated/stored; millimeter imaging technology that see through clothes (Surette, 2005); networked sensors that can monitor people's eye movements, body heat, etc.; and finally multiple chemical, biological, and radiological sensors (Canantaci, 2010). These enhancements and the integration of other technologies are part of the evolution from first-generation CCTV systems to second-generation systems, in order to address the problems, weaknesses and deficiencies of the earlier systems (Surette, 2005).

The integration of a variety of sensors (audio sensors and chemical, biological, and radiological sensors) with CCTV technology has been categorized in Europe as "Massively Integrated Multiple Sensor Installations" (MIMSI) (Cannataci, 2010). In the US, the term for MIMSI is "Domain Awareness System" (DAS) (*Ibid.*). The New York Police Department (NYPD) defines DAS as "technology deployed in public spaces as part of the counterterrorism program of the NYPD's Counterterrorism Bureau".[316] As Cannataci (2010) shrewdly points out, the NYPD's broad definition of DAS clearly allows for practically any type of technology (device, sensor, etc.) to be integrated.

As part of the increasing enhancement of public surveillance capabilities, highly sensitive omni-directional microphones and (horn) loudspeakers have been integrated into public space CCTV surveillance systems in the UK. This enhancement phase of public space CCTV surveillance systems, which this dissertation principally addresses, is the present move beyond the collection of images to the capability of both recording and communicating audio data with the addition of microphones and loudspeakers respectively.

The increasing integration of additional surveillance technologies with existing CCTV surveillance technology can significantly expand the threat to privacy (Cannataci, 2010). Accordingly, the increase in a surveillance system's capabilities increases the need for additional relevant policies (Surette, 2005, p. 164). The integration of microphones and loudspeakers with CCTV cameras equally requires corresponding policies and regulations to ensure the adequate protection of privacy and liberty.

[316] NYPD's Public Security Privacy Guidelines, 2 April 2009, p. 2, available at: http://www.nyc.gov/html/nypd/downloads/pdf/crime_prevention/public_security_privacy_guidelines.pdf

6.3 THE EARS AND MOUTH OF 'BIG BROTHER'

Indeed, an era is emerging where practically any individual, and not only governments or large corporations, can engage in activities that intrude upon the privacy of many, as a result of the widespread accessibility and use of advanced technology.[317] In addition, rogue individuals with special computer skills can hack into people's personal computers and mobile phones. Nevertheless, any notion that the infamous 'Big Brother' metaphor is already outdated, as a result of the existence of so-called "small brothers", is still somewhat premature.

In the UK especially, the actions and policies of the British Government have done well to keep 'Big Brother' alive and kicking.[318] In George Orwell's *Nineteen Eighty-Four*, "telecreens" – two-way screens complete with microphones and loudspeakers – surrounded the masses in fictional "Oceania", in order to monitor and control their behaviour both in their homes and in public spaces. With the equivalent of eyes, and now also the equivalent of ears (microphones) and a mouth (loudspeakers), in a matter of speaking, there are valid concerns that CCTV cameras have become much closer to resembling the telescreens of Oceania and have further become an incarnation of 'Big Brother'.

Both CCTV loudspeakers and CCTV microphones could, therefore, reinforce the ability of CCTV cameras to monitor and control public behavior "through the promotion of habituated anticipatory conformity" (Norris and Armstrong, 1999, p. 5). Like in *Nineteen Eighty-Four*, where people assumed that every sound was overheard and movement observed (Orwell, 1949, p. 9), the known presence of CCTV loudspeakers and microphones could lead to not only direct social control, but their perceived presence could wreak indirect control. As Hubert H. Humphrey once observed, "[i]f we can never be sure whether or not we are being watched and listened to, all our actions will be altered and our very character will change".[319] In the words of Foucault, "an inspecting gaze, a gaze which each individual under its weight will end up interiorizing to the

[317] For example, with a smartphone an ordinary individual can broadcast live videos onto USTREAM and with an iPhone can even control a small flying drone (developed by Parrot) that has a video-streaming camera. Moreover, hundreds of millions of people are walking around with a smartphone video camera and they can easily and immediately upload their videos onto YouTube.

[318] The UK Government's plan to install 24-hour CCTV systems in the homes of 20,000 selected families to tackle anti-social behavior is yet another reason why the 'Big Brother' metaphor is still valid. In addition, hundreds of CCTV cameras have already been deployed within housing trusts across the UK. see Little, Alison. "Sin bins for worst families" (Daily Express, 23 July 2009), available at: http://www.express.co.uk/posts/view/115736

[319] see Long, Edward V. *The Intruders: The Invasion of Privacy by Government and Industry* (Praeger, 1967), viii.

point that he is his own overseer, each individual thus exercising this surveillance over, and against himself" (Foucault, 1980, p. 155).

Public space CCTV cameras can already bring about the similar panoptic feelings caused by Jeremy Bentham's 'panopticon' design (Bannister et al., 1998). When people have panoptic feelings, they often increasingly adjust their behaviour to comply with what society considers 'normal' or socially acceptable (Schermer, 2007, pp. 217-18). Panoptic feelings may affect greater those who are more aware of the possibility (Schermer, 2007), whether real or potential, that they are being observed, especially if they are reminded of this possibility via CCTV loudspeakers. Attaching both loudspeakers and microphones to CCTV cameras will thus likely only increase the power of CCTV cameras to cause panoptic feelings in the long-term.

6.3.1 The ears (microphones)

Whether over the phone or face-to-face, conversations were beforehand considered private. Today, phone calls can be potentially monitored, and mobile phones (even when turned-off) and computers can be used as an eavesdropping device, while conversations have moved to online instant messaging, which can also be monitored and digitally stored. With the further advancement of listening devices[320] and the continuous evolution of privacy invasion, face-to-face conversations out in public are now potentially the latest target.

The ongoing attachment of microphones to CCTV cameras in the UK, at present, permits the recording of audio data in combination with video data to give a near complete account of activities in the public space(s) concerned. As Steve Harrison, Westminster's Assistant Director of Community Protection asserts, concerning the attachment of microphones to CCTV cameras in Westminster, "[t]his is about trying to instantly capture an image and audio that goes with it to let us know what's going on".[321] The CCTV microphones are reportedly so sensitive that they can provide CCTV control room operators the capability to potentially monitor and record conversations out in public many meters

---

[320] Revolutionary technology in electronic eavesdropping includes the use of devices that transmit laser beams or very high frequency radio waves, which can enable users to listen in to a conversation hundreds of feet away and practically render windows and/or walls invisible.

[321] Derbyshire, David. "Council plans to listen in on street life" (The Telegraph, 4 May 2005), available at: http://www.telegraph.co.uk/news/uknews/1489282/Council-plans-to-listen-in-on-street-life.html

from their location source. This would also raise concerns over the potential for CCTV microphones to possibly record conversations within private homes.[322]

Understandably, individuals often discuss personal thoughts or feelings during their verbal interactions out in public, including political opinions, religious beliefs or other beliefs of a similar nature, which Section 2 of the Data Protection Act 1998 legally recognizes as "sensitive personal data". Although these verbal discussions may occur out in public, they still arguably merit a reasonable expectation of privacy, albeit if kept at a certain volume level,[323] and should not be recorded by public or private bodies. While video surveillance of the general public obviously cannot listen in and record these opinions, feelings or beliefs when expressed verbally, the attachment of microphones to public space CCTV cameras, on the other hand, can provide the audio recording capability necessary to do so.

CCTV microphones could equally jeopardize certain individual liberties and fundamental freedoms, and repress legitimate political dissent, all in the name of security, similar to other technologies capable of mass surveillance (Cockfield, 2003). For instance, CCTV microphones could have the so-called "chilling effect"[324] on the freedom of expression, as people become more cautious of what they express with their friends and family out in public. Governments could even use CCTV microphones to monitor what is being said during a protest or what people generally talk about as means of becoming better aware of public opinion and maintaining political and social control.

On top of that, the audio data collected by CCTV microphones, in conjunction with the video data collected by the cameras, could be used not only to further monitor and control behavior in public spaces, but even also to enforce anti-social behavior rules concerning excessive noise at housing areas under the Anti-social Behaviour Act 2003 and the Crime and Disorder Act 1998. Local governments have already used

---

322 There have already been concerns over the deployment of CCTV cameras positioned in a way that can view inside the windows of private homes.

323 However, perhaps this expectation of privacy could one day be forgotten, as today's Internet generation (or Generation I or Generation Z) have a growing expectation, or even desire, to communicate to an audience what most would traditionally view personal. see Nussbaum, Emily. "Say Everything", Kids the Internet, and the End of Privacy: The Greatest Generation Gap Since Rock and Roll (New York Magazine, 12 February, 2007), available at: http://nymag.com/news/features/27341/

324 A legal term predominantly adopted in US courts, which is used in reference to laws, circumstances or actions that do not explicitly prohibit the exercise of fundamental freedoms, but rather bring about unnecessary repression or an intolerable burden on exercising these freedoms. The term has also been increasingly recognized and referred to by the ECtHR on numerous occasions. see, for example, *Case of Kyprianou v. Cyprus*, Application no. 73797/01, Judgment of 15 December 2005, para. 175: *Steel and Morris v. UK*, Application no. 68416/01, Judgment of 15 February 2005, para. 95; *Case of Wille v. Liechtenstein*, Application no. 28396/95, Judgment of 28 October 1999, para. 50.

CCTV cameras deployed in housing areas to monitor individuals subject to Anti-Social Behaviour Orders (ASBO) or Acceptable Behaviour Contracts (ABCs) and to gather information and evidence in certain locations for an ASBO application.[325] The policy and strategy is thus already potentially in place for using CCTV microphones for the similar purposes.

6.3.2 The mouth (loudspeakers)

Public CCTV loudspeakers primarily concern the component of privacy that endows citizens the right to be left alone. The loudspeakers attached to public CCTV cameras provide their operators the capability not only to observe people in public, but also to scold individuals and shout commands at them. While there are other methods in which CCTV operators can disturb individuals,[326] with the widespread deployment of CCTV loudspeakers, the scope of the ability to do so is unprecedented.

The deployment of CCTV loudspeakers is (or at least was) part of the UK Government's 'Respect Action Plan', a scheme for tackling anti-social behavior or low-level crime.[327] In the words of the Home Office, the use of the "talking cameras", as the Home Office and media refers to them, is to "tackle bad behaviour and promote good".[328] Any individual who engages in an activity considered by the CCTV operator to be "bad behavior" or "anti-social" can potentially be scolded and publicly humiliated or ridiculed into behaving "correctly". CCTV loudspeakers are thus being used as a means of threatening public humiliation, in order to deter anti-social behavior, which may be a form of social control through the conveyance of informal punishments, as opposed to social control through the threat of formal sanctions, such as fines or imprisonment.

While most people may likely not have a problem with CCTV loudspeakers, if their use prevents the vandalizing of property or leads to safer and cleaner streets and

---

325 see "Tackling Anti-Social Behaviour in Mixed Tenure Areas", Office of the Deputy Prime Minister, March 2003, p. 104, available at: http://www.communities.gov.uk/documents/housing/pdf/138706.pdf

326 For example, a CCTV control room operator could bother people he or she sees using public telephone booths. see "Phone Pest picked targets on security video" (The Telegraph, 7 June 1996), available at: www.telegraph.co.uk/html-Content.jhtml?html=/archive/1996/11/27/ntel27.html

327 see the Respect Action Plan, produced by the Central Office of Information on behalf of the Respect Task Force (based in the Home Office), January 2006.

328 see a promotional image from the Home Office, available at: http://www.respect.gov.uk/uploadedImages/Public_site/Homepage/Main_features/TalkingCCTVbanner428x161.jpg

parks, however, once the public accepts CCTV loudspeakers, their deployment could become further routine. Today, CCTV loudspeakers are largely being used to discourage vandals or fly tippers. But, eventually the widespread, unregulated deployment and use of CCTV loudspeakers could lead to a new echelon of social control.

Rather than using restricted pre-recorded messages, operators have the ability to speak directly to individuals from afar. The CCTV loudspeakers in their present form effectively grant their operators the power to intrude upon the daily lives of ordinary people and disturb the right to be left alone. Without technological or legal limitations as to what can be said, when, where and for which purposes, the potential for CCTV operators to abuse the intrusive capability of loudspeakers is immense. There is essentially nothing to prevent operators from yelling out demeaning statements. Accordingly, the attachment of loudspeakers to CCTV cameras could further threaten personal freedom and personal dignity.

The use of CCTV loudspeakers to tackle anti-social behaviour and/or crime might be just the beginning. As John Willman suggests, an editor of the *Financial Times*, CCTV loudspeakers could be used to greet customers and tell them about new products and special offers, and, with the addition of improved face recognition technology or the development and integration of highly-advanced iris scanners,[329] CCTV loudspeakers could direct these messages to identified customers, much like the personalized talking advertisements in Steven Spielberg's film *Minority Report*.[330] In addition, CCTV loudspeakers could also be used by employers to convey work-related commands to employees and by schools to scold students who break the rules.

Moreover, the 'asymmetrical' design of CCTV loudspeakers, as a result of the inability of the general public to verbally respond to the speaker (i.e. the CCTV loudspeaker operator), in addition to not being able to see him or her, could exacerbate the unequal relationship between the observers (CCTV control room operators) and the observed (general public) (for further discussion, see, e.g., Hubbard et al., 2004, p. 244).

---

[329] Iris scanners could rapidly advance, as a result of an innovation, known as Smart-Iris, developed from the ultra high-resolution, ultra-thin, lens-free, Panoptes cameras merged with projection devices. The advancement could remove the problems associated with traditional iris scanners, such as glare, dim lighting and the need for cooperative individuals to stop and stare at the scanners. see Drummond, Katie. "Darpa's Beady-Eyed Camera Spots the 'Non-Cooperative'" (Wired, 27 May 2010), available at: http://www.wired.com/dangerroom/2010/05/darpas-beady-eyed-camera-spots-the-non-cooperative/

[330] see John Willman, "Talking cameras are just the start" (Financial Times, 7 April 2007), Ed1, p. 9.

6.4 SCOPE OF DEPLOYMENT IN THE UK

CCTV microphones and loudspeakers, for the most part, are being deployed in the UK alone.

6.4.1 CCTV microphones

Westminster City Council began testing CCTV microphones in 2005 to deal with noise at night,[331] but later reportedly decided not to proceed further.[332] Regardless, apparently more than 300 public CCTV cameras have been fitted with microphones in benefit offices and city centers.[333] For example, the public should be aware that a CCTV microphone is apparently located on Riverside Road near the Wimbledon Stadium, since the media reported that this particular CCTV microphone recorded a suspect's "manic" laughter nearby a crime scene.[334] Nevertheless, the extent to which CCTV microphones have been deployed is not clear. The BBC reported on a controversial proposal to use CCTV microphones on crowds during the 2012 Olympic Games in London,[335] in addition to the estimated 500,000 CCTV cameras the police plan to use.[336]

The increasing deployment of wireless network infrastructure in urban public spaces helps to reduce the costs of setting up and operating CCTV microphones. Moreover, audio data does not require an excessive amount of additional storage space. Therefore, due to the relatively simple installation of CCTV microphones and inexpensiveness and availability of the technology, their widespread deployment is not inconceivable.

---

331 Iain Thomson, "Council listens in to Soho crowds" (Vnunet, 4 May 2005), available at: http://www.vnunet.com/vnunet/news/2127273/council-listens-soho-crowds

332 Iain Thomson, 'Westminster Pulls CCTV Microphones' (Vnunet, 31 January 2008), available at: http://www.vnunet.com/vnunet/news/2208582/westminster-pulls-cctv

333 see statement made by Baroness Walmsley, Daily Hansard for 12 June 2008, Volume No. 702, Part No. 106, Column 736, available at: http://www.publications.parliament.uk/pa/ld200708/ldhansrd/text/80612-0010.htm

334 The man is no longer a suspect in the murder. see Harding, Eleanor. "Mystery chuckler not the killer of Andrew Cunningham from Earlsfield" (Local Guardian, 4 June 2009), available at: http://www.yourlocalguardian.co.uk/news/local/wimbledonnews/4419573.Mystery_laughter_leads_to_dead_end/

335 John Pienaar, 'Olympics audio surveillance row' (BBC News, 26 November, 2006), available at: http://news.bbc.co.uk/1/hi/uk_politics/6186348.stm

336 "CCTV plan to boost 2012 security" (BBC News, 4 March 2008), available at: http://news.bbc.co.uk/2/hi/uk_news/england/london/7278365.stm

The SIgard system, developed by Sound Intelligence,[337] was set up in London, Manchester and Coventry[338] and tested in Glasgow.[339] The CCTV microphones are linked to computers with sound analysis software and are apparently able to determine when sound contains the indicators of aggression (similar to the way the human brain interprets sound) and then alert the CCTV operators.[340] The CCTV microphones that were installed in Westminster were activated if noise levels reached above a certain threshold and made use of the existing Wi-Fi network that links the cameras to Westminster's central CCTV control room.

6.4.2 CCTV loudspeakers

A freedom of information request could reveal precisely how many loudspeakers have been connected to CCTV cameras throughout the UK and, if their use is indeed being tracked, how many times they have been used and precisely for which reasons.[341]

CCTV loudspeakers were first pioneered in Wiltshire in 2003.[342] As part of a special initiative called "Fancy an early night?", CCTV loudspeakers were deployed

337 A Netherlands based company, specializing in the development of advanced technology for the detection and analysis of sound. Sound Intelligence, available at: http://www.soundintel.com

338 W. van Reijendam. "English Bobbies can escape the normal life by listening to aggression detection" (Financieel Dagblad, 13 May 2008), available at: http://www.soundintel.com/en/nieuws/algemeen/groningse-camera-hoort-agressie.html

339 see Macdonald, Kenneth. "CCTV cameras 'listen for trouble'" (BBC News, 13 February 2009), available at: http://news.bbc.co.uk/2/hi/uk_news/scotland/7886656.stm

340 Sound Intelligence, available at: http://www.soundintel.com

341 I sent an identical freedom of information request by email on 14 November 2008 to the Home Office. An official reply from the Home Office was received on 26 November 2008 stating that the matters raised in the request are the responsibility of the Communities & Local Government and that the request has been transferred accordingly. After several weeks and not receiving further information, I inquired with the Communities & Local Government and resent my request on 3 March 2009. I was informed within 20 days that my previous request could not be traced, but that I would receive a response to my original request by 2 April 2009. On 27 March 2009, I received the FINAL response (Ref: F0002996) informing me that despite enquiries made of a number of the Business Units, the information I requested could not be provided since the Communities and Local Government does not hold this information. It was suggested that I contact the relevant local authorities or the particular police forces. What I have learned from this process is that either the UK Government does not want to provide this information or worse that indeed the use and deployment of CCTV loudspeakers is not being tracked centrally, if it is even being tracked at all. I can only hope it is being tracked locally.

342 "Talking CCTV pioneered in Wiltshire" (BBC News, 23 May 2003), available at: http://news.bbc.co.uk/2/hi/uk_news/england/wiltshire/2933626.stm

three years later in Middlesbrough Borough. More than a dozen CCTV loudspeakers have been fitted to public space cameras in Middlesbrough. Subsequently, on 4 April 2007, it was announced that loudspeakers would be fitted to numerous CCTV cameras in the following additional 20 areas, boroughs, cities or towns across the UK: Blackpool, Barking and Dagenham, Coventry, Darlington, Derby, Gloucester, Harlow, Ipswich, Mansfield, Northampton, Norwich, Nottingham, Plymouth, Reading, Salford, Sandwell, Southwark, South Tyneside and Wirral.[343] The announcement has been followed through.

CCTV loudspeakers are not only being deployed in city or town centers, but within parks and at hospitals. In Norwich, loudspeakers were fitted to multiple cameras in Waterloo Park and Eaton Park in order to curb littering.[344] In Wolverhampton, New Cross Hospital installed CCTV loudspeakers to scold people for failing to use designated smoking areas.[345]

The deployment is being funded through the Respect Task Force,[346] while the CCTV loudspeakers are being installed by local authorities, in partnership with the local police department and in coordination with the Home Office and local anti-social behaviour coordinators.

According to a statement made by Vernon Coaker, the Minister of State responsible for policing, crime and security at the Home Office, "the [Respect] task force has no current plans to fund further roll-out to other areas".[347] However, this does not mean that CCTV loudspeakers will not be deployed in more and more towns and cities with further funding from other sources. Since then, several additional towns have already followed suit. For example, Bristol subsequently initiated a three-month pilot[348] and

343 see "Children remind adults to act responsibly on our streets", Home Office, 4 April 2007, available at: http://www.asb.homeoffice.gov.uk/news/article.aspx?id=10310

344 "Offenders warned by talking CCTV" (BBC News, 13 April 2007), available at: http://news.bbc.co.uk/2/hi/uk_news/england/norfolk/6551501.stm

345 "Talking CCTV' to tackle smokers" (BBC News, 31 July 2008), available at: http://news.bbc.co.uk/1/hi/england/west_midlands/7535927.stm

346 The Respect Task Force is an inter-ministerial steering group, established in 2005, with the direct responsibility over the UK Government's 'Respect' agenda.

347 Daily Hansard for 10 May 2008, Column 427W, available at: http://www.publications.parliament.uk/pa/cm200607/cmhansrd/cm070510/text/70510w0019.htm

348 "City pilots 'talking' CCTV", 10 December 2007, available at: www.bristol.gov.uk/redirect/?oid=PressRelease-id-21982088

Hartlepool also announced their plans to tryout CCTV loudspeakers.[349] Merseyside, a metropolitan county, which includes the City of Liverpool, plans to dismantle thousands of old lampposts and replace them with new high-tech CCTV equipped ones. The new lampposts will reportedly include loudspeakers.[350]

CCTV loudspeakers are also being funded, deployed and operated by private entities. The Leeds-based property developer, Business Homes, have installed what they dub as "a state-of-the-art audio CCTV system" at the business park Halbeath Interchange in Dunfermline and are installing the system on all 25 of the business parks the company is currently developing throughout the UK.[351] McDonald's also deployed at 20 restaurants across the UK a system of CCTV cameras fitted with both microphones and loudspeakers, which are monitored and controlled via a central control room.[352]

The installation of the CCTV loudspeaker systems currently in place in Middlesbrough, West Bromwich and Nottingham, and supplied by Complus Teltronic, utilize the existing fiber optics or communications infrastructure.[353] With the Apex system, however, all information is sent and received via radio waves. Each unit integrated into the CCTV network is composed of a horn loudspeaker, small antenna, radio receiver, transmitter and power supply unit, and has a unique identification number. The CCTV control room can operate the units several kilometres from where the actual CCTV cameras and loudspeakers are located. By entering the unit's identification number and pressing the activation button, the operator can activate the corresponding loudspeaker.[354] Similarly, MEL Secure Systems launched CCTV loudspeaker systems that are ready to install and use digital wireless transmission. The loudspeakers of Bosch Secu-

---

349 "Talking cameras coming soon..." (Hartlepool Mail, 3 October 2008), available at: http://www.hartlepoolmail.co.uk/news/Talking-cameras-coming soon.4556556.jp

350 Coligan, Nick. "CCTV on every corner" (Liverpool Echo, 29 November 2007),

351 "Business Park's Talking CCTV A 'First' for Fife'", Business Homes, 1 September 2007, available at: http://www.businesshomes.com/newsDetails.asp?id=60

352 SourceSecurity.com, available at: http://www.sourcesecurity.com/markets/retail-and-eas/application/co-73-ga.350.html

353 "Talking CCTV Cameras – Middlesbrough", Complus Teltronic, 13 April 2007, available at: http://www.complusteltronic.co.uk/eng/newsdetail.asp?ID=396

354 Apex Radio Systems Ltd., available at: http://www.apexradio.co.uk/talkingcctv.php

rity Systems, on the other hand, apparently have superior sound quality, and have been deployed, for example, in Plymouth city for that reason.[355]

At this rate and level of enthusiasm, there is little reason to believe that CCTV loudspeakers will not eventually be deployed in every major town or city in the UK, and beyond. As a demonstration of what potentially is to come, CCTV loudspeaker technology was displayed at the 2007 Milipol exhibition, the world's largest for internal state security technology.[356] Given the relatively quick and easy installation of CCTV loudspeakers and integration with existing CCTV surveillance systems, the greater widespread deployment of CCTV loudspeakers is also not inconceivable.

6.5 SECURITY GAINS

The public security gains of integrating microphones and loudspeakers to CCTV cameras are centered mostly on their potential to enhance the ability of CCTV control room operators to do their job, which is to assist in the fight against crime and terrorism.

6.5.1 CCTV microphones

CCTV cameras are meant to help ensure public safety, i.e. to prevent crime and help counter-terrorism activities. Indeed, the UK Home Office has spent an overwhelming amount of its crime prevention budget on installing CCTV cameras. However, there is insufficient empirical evidence that CCTV cameras are helpful in preventing or reducing crime, which raises questions on their legitimacy and whether or not the deployment and use of CCTV cameras is proportional and justified. A Home Office report concluded that of the 14 CCTV systems it assessed, "most systems revealed little overall effect on crime levels […]."[357] Even more, CCTV cameras have shown to be more effective for reducing property crimes than violent crimes (Welsh and Farrington, 2003-2004, pp. 513-14) or preventing vehicle crimes in car parks. There is also little reason

355 "Bosch delivers CCTV with loudspeakers to Plymouth City", Security World Hotel, 5 May 2007, available at: http://www.securityworldhotel.com/int/news.asp?string1=&string2=&string3=&string4=&YearSearch=2007&category=0&company_id=&NAV=2&id=38223

356 see "Paris - Milipol to Focus on Homeland Security", Intelligence Online, 4 October 2007.

357 Martin Gill, Angela Spriggs et al., "The impact of CCTV: fourteen case studies", Home Office Online Report 15/05, p. 34, available at (last time visited: 23/01/12): http://www.homeoffice.gov.uk/rds/pdfs05/rdsolr1505.pdf

to believe that CCTV cameras significantly aid in criminal investigations. As Detective Chief Inspector Mick Neville asserted in May 2008 at a Conference of the Metropolitan Police's Visual Images Identifications and Detections Office (Viido), although "billions of pounds has been spent on kit" […], "only 3% of crimes were solved by CCTV"[358]. Moreover, an internal Scotland Yard report stated that less than one crime is solved per year for every 1,000 CCTV cameras in London, and there over a million CCTV cameras in London alone (Cannataci, 2010).[359] Therefore, CCTV cameras are not an effective alternative to traditional policing methods and activities and training and deploying more police officers.

Public space CCTV systems especially require human operators to be vigilant and sharp-eyed, in order to effectively observe multiple screens in real-time (or multiple video streams displayed on a single screen simultaneously). Often these images include areas with many persons, objects and activities present. The effectiveness of CCTV cameras is, thus, significantly dependent on the performance of operators, which can also degrade over time due to boredom or fatigue (Smith, 2004; Surette, 2005) or loss of concentration (Cannataci, 2010) and other 'human factors'. There are also a limited number of CCTV control room operators and, at times, the real-time video streams may go unmonitored (Norris and Armstrong, 1999). In addition, CCTV cameras naturally can only observe events, persons or objects within their field of view, which may occasionally be obstructed, for instance, by trucks or trees, or may even be impossible to view.

Although there is equally no empirical evidence proving so, combining microphones with public space CCTV cameras could improve the performance of the CCTV operators and perhaps even reduce the number of CCTV operators needed and/or improve the efficiency of their employment/deployment, which during the current ongoing economic crisis is becoming crucial.[360] CCTV microphones could also significantly enhance the capability of the CCTV cameras to detect crime. As Kim et al. demonstrate, auditory sensors can shorten the time required to locate a specific object, whereby the ability of humans to locate the direction of a sound's source can be mimicked by machines (2007, p. 383).

---

358 "CCTV boom failing to cut crime" (BBC News, 6 May 2008), available at: http://news.bbc.co.uk/2/hi/uk_news/7384843.stm

359 Hickley, Matthew. "CCTV helps solve just ONE crime per 1,000 as officers fail to use film as evidence" (The Daily Mail, 25 August, 2009), available at: http://www.dailymail.co.uk/news/article-1208700/CCTV-helps-solve-just-ONE-crime-1-000-officers-fail-use-film-evidence.html

360 see Camber, Rebecca. "Big brother is NOT watching you: Cash-strapped towns leave CCTV cameras unmonitored" (Daily Mail, 16 December 2008), available at: http://www.dailymail.co.uk/news/article-1095609/Big-brother-NOT-watching-Cash-strapped-towns-leave-CCTV-cameras-unmonitored.html

Sound is omni-directional as opposed to vision, which is directional, and, unlike vision, sound is not negatively affected by poor lighting or entirely obstructed by obstacles. Microphones can provide CCTV systems and operators the ability to detect crime beyond a camera's field of view and can help them to work better in areas with insufficient light. If several microphones are installed at a certain distance from each other, the location of the sound source can automatically be determined, based on the time difference of the arrival from the sound source to the sensors (Kim et al., 2007, p. 384). A pan/tilt/zoom (PTZ) CCTV camera can be pointed in that direction and the operator can simultaneously be both audibly and visibly alerted to contact the police immediately via a wireless network. CCTV microphones can therefore enhance the vigilance and effectiveness of CCTV operators and help them to observe more monitors or video streams, without having to hopelessly attempt to watch each simultaneously at all times. The SIgard system is based on the premise that violent incidents supposedly often start with verbal aggression or shouting, without actually conveying this so-called evidence.[361] While shouting may not justify triggering the CCTV microphones, gunfire, broken glass and explosions certainly do.

CCTV microphones can also potentially provide evidence in a court of law. For instance, the groans of Mark Witherall, while he was being brutally beaten and left to die by thieves, were recorded by a neighbor's security camera, which had audio recording capability, and was used as evidence against the offenders during the criminal trial.[362] In this case, however, microphones attached to public space CCTV cameras were not the source of the evidence, but rather the audio capabilities of security cameras in a private home.

6.5.2 CCTV loudspeakers

CCTV cameras, for the most part, do not prevent or deter crime, but rather simply record the criminal event, since there is a limited number of CCTV control room operators and the operators are not able to do much more beyond contacting the police or sounding an alarm. These deficiencies of CCTV cameras could perhaps be countered by the use of loudspeakers. The argument is that CCTV loudspeakers could potentially be used to combat crime and anti-social behaviour at an early stage by confronting

[361] Sound Intelligence, available at: http://www.soundintel.com

[362] "Teenagers could be heard on CCTV as they murdered father of three" (Daily Mail, 17 January 2008), available at: http://www.dailymail.co.uk/news/article-508880/Teenagers-heard-CCTV-murdered-father-three.html

those who engage in such acts, issuing warnings and reminding people that they are being monitored. In the words of Graeme Gerrard, the Chair of the CCTV Working Group of the Association of Chief Police Officers (ACPO) and Deputy Chief Constable of Cheshire Police:

> Talking CCTV [CCTV loudspeakers] increases the effectiveness of town centre cameras because it allows the camera operators to intervene and let the offender know their anti-social behaviour has been spotted and is being recorded. In many cases this is enough to stop the offending behaviour which in turn results in safer and tidier streets.[363]

CCTV operators could use the loudspeakers to swiftly intervene and discourage or dissuade unlawful or violent behaviour in real time, or perhaps even before it happens, and to warn someone if danger approaches them. For example, the technology was used as a deterrent at Business Homes' Nottingham site earlier this year against would-be thieves.[364] In addition, CCTV loudspeakers could also be used to reassure someone who requires immediate medical attention that emergency services have been contacted and are on their way.

According to Middlesbrough Council's security manager, Jack Bonnar, the town had recorded a 65-70% reduction of public order offences, such as disorderly conduct, since the introduction of CCTV loudspeakers.[365] Moreover, Middlesbrough Councilman Barry Coppinger asserts that CCTV loudspeakers have "raised awareness that the town centre is a safe place to visit and also that we are keeping an eye open to make sure it is safe".[366] Other places, such as Ipswich, have also reported a success.[367]

Once again, however, anti-social behaviour, such as littering, dog fouling, public urinating, or loitering, can hardly be considered threats to public safety, which calls

---

363 see "Children remind adults to act responsibly on our streets", Home Office, 4 April 2007, available at: http://www.asb.homeoffice.gov.uk/news/article.aspx?id=10310

364 see "Business Park's Talking CCTV A 'First' for Fife'", Business Homes, 1 September 2007, available at: http://www.businesshomes.com/newsDetails.asp?id=60

365 see "Children remind adults to act responsibly on our streets", Home Office, 4 April 2007, available at: http://www.asb.homeoffice.gov.uk/news/article.aspx?id=10310

366 "Talking' CCTV scolds offenders" (BBC News, 4 April 2007), available at: http://news.bbc.co.uk/2/hi/uk_news/england/6524495.stm

367 "TALKING CCTV cameras are set to stay in Ipswich after a trial proved a success,...", (Evening Star, Ipswich, 20 June 2008).

into question whether or not CCTV loudspeakers should be used to prevent or inhibit these acts and, if so, to what extent. After all, these acts have more than likely occurred millions of times in the UK alone. On the other hand, more serious forms of anti-social behaviour or disorderly conduct, such as vandalism, undoubtedly do pose a more serious threat to public safety and well-being. Nevertheless, the use of CCTV loudspeakers to prevent or deter lower level anti-social behaviour could, in theory, free police to fight real crime by reducing avoidable bureaucracy and paperwork.

Still, the effectiveness of CCTV loudspeakers in improving public safety or reducing anti-social behaviour has yet to be thoroughly evaluated or credibly proven. Moreover, if the commands broadcasted from CCTV loudspeakers are not respected and not enforced then their effectiveness will depreciate overtime until they most likely end up useless. In Salford Council, for instance, over half of the people reprimanded in 2007 for their behaviour via the CCTV loudspeakers ignored the reprimand.[368] On the other hand, in Nottingham, of the 109 people spoken to by CCTV operators using the loudspeakers, 78 did what they were told, and in 16 cases operators called a police officer to the scene and 12 fines were issued as a result.[369]

Nonetheless, the widespread deployment of CCTV loudspeakers could eventually incite rebellious acts in response, if it has not already, which could then result in more anti-social behavior than there was before.

6.6 ALTERNATIVES TO THE CCTV MICROPHONES AND LOUDSPEAKERS DEPLOYED IN THE UK

There are indeed a number of more privacy-friendly alternative devices and/or means, already in existence, with the purpose of helping to prevent and reduce crime and anti-social behaviour.

6.6.1 CCTV microphones

Gunfire and explosive detection systems have been around for more than ten years (Mazerolle et al., 1999). The ShotSpotter™ system, which the local police department

[368] Haris, Jan. "Most people ignore talking CCTV", CCTV Core, available at: http://www.cctvcore.co.uk/27-09-2007-most-people-ignore-talking-cctv.html

[369] "Talking CCTV a success in the city" (Nottingham Evening Post, 5 August 2008).

began operating in Redwood City, California as early as 1995, uses strategically placed sensors or microphones to triangulate the location of gunfire across wide areas within seconds of a weapon being fired (Monmonier, 2004, pp. 116-119). The ShotSpotter™ system has demonstrated accuracy within 25 meters. In addition, ShotSpotter™ can support subsequent forensic analysis, including the type of gun used, the direction of the gunfire, and even information related to the direction and speed of shooters on the move.[370] During the 2004 Olympic Games in Athens, pole-mounted microphones were used to detect explosions and gunfire and quickly pinpoint the location of an incident.[371]

6.6.2 CCTV loudspeakers

Derwent has developed a system, which detects trespassers and then automatically issues a warning over loudspeakers to leave the area. At night, the system's powerful AEGIS White Light LED illuminators, activated by a passive infra-red (PIR) sensor, can flood the area with light.[372] It is not hard to imagine that a sudden burst of bright light will deter trespassers and vandals.

A similar device called FlashCAM-880 developed by Q-Star Technology automatically takes a digital photo and delivers a recorded message, when activated by motion sensors, to deter intruders, vandals, graffiti taggers or illegal dumpers. The digital camera can operate in total darkness and has an operating range of up to 100 feet. FlashCAMs have been deployed in cities throughout the US and have resulted in a number of success stories.[373]

An additional alternative device to CCTV loudspeakers is the Mosquito™, an anti-vandal system developed by Compound Security Systems Ltd., which emits a high frequency sound that is piercing only for teenagers. The Mosquito™ has proven to successfully drive away gangs of youths and in doing so can prevent teenagers from

370 ShotSpotter, Inc., available at: http://www.shotspotter.com/products/technology.html

371 'Olympian challenge', Info4 Security, 5 February 2007, available at: http://www.info4security.com/story.asp?storyCode=3093811&sectioncode=16

372 "Derwent's White Light Illuminators Tackle Network Rail Thieves", Derwent, available at: http://www.derwentcctv.com/home/index.php?id=7&nid=75

373 Q-Star Technology, available at: http://www.qstartech.com

engaging in acts of vandalism or loitering in front of businesses. The Mosquito™ has been deployed throughout the UK.[374]

The so-called "Manilow Method", whereby opera, classical or other music unpopular with teenagers is played to drive away youth, has also been used in the UK by shop owners and local councils, reportedly with some success.

Improved street lighting is another alternative to the increased deployment of CCTV cameras. Research has also shown that improved street lighting in a public space setting leads to a greater reduction in overall crime than CCTV cameras (Welsh and Farrington, 2003-2004, p. 513).

The further recruitment and deployment of Police Support Community Officers (PSCOs) or other authorized officers of a local authority or security operatives licensed by the Security Industry Authority, is an additional alternative to the use of CCTV loudspeakers in tackling anti-social behaviour. Whether deploying more human resources on the ground is more effective than using CCTV loudspeakers is debatable, but certainly this method reduces the concerns of 'asymmetric' observation (see Hubbard et al., 2004) and any unnecessary/inappropriate public humiliation.

Other alternatives to CCTV loudspeakers and their approach to 'correcting' anti-social behavior through near public humiliation, are education and after-school social programs, and even video games, such as the interactive gaming technology platform developed by Project rePLAY through EU funding.

6.7 LAWS, CODES AND OTHER LEGAL/POLICY INSTRUMENTS OF SPECIAL RELEVANCE IN THE UK

As widely recognized, CCTV surveillance systems may legitimately be deployed for the sake of preventing and detecting crime, protecting property and individuals, and defending public interests.[375] The police are especially permitted to use CCTV systems for carrying out their duties and functions. Other public entities and private entities may also be permitted to use CCTV cameras, since their use may be considered reasonable to prevent criminal offenses or assist in the lawful arrest of offenders. Consent is not required, since the collection and processing of the data from CCTV surveillance sys-

---

374 Compound Security Systems, available at: http://www.compoundsecurity.co.uk

375 see Article 29 Working Party, Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance (WP 89).

tems is deemed necessary to protect the vital interests of society and to prevent threats to public safety/security, when carried out in accordance with the law.

In the opinion of the Article 29 Working Party, Directive 95/46/EC applies to the processing of image and sound data by means of CCTV surveillance systems.[376] The Data Protection Act 1998 (DPA) implements or transposes in its own way Directive 95/46/EC into UK domestic law.

In short form, the eight data protection principles, listed in the DPA,[377] requires that all personal data must be:

- Processed fairly and lawfully;
- Obtained and used only for specified and lawful purposes;
- Adequate and relevant, and not excessive;
- Accurate and, where necessary, up to date;
- Kept no longer than necessary;
- Processed in accordance with the rights of individuals;
- Secure; and
- Transferred only to third-party countries that have adequate data protection laws and practices

Once again, these data protection principles are parallel to the principles of privacy outlined in Chapter 3. The first data protection principle, and the conditions that must be met in accordance with Schedules 2 and 3 of the DPA, are basically parallel to the principle of consent/choice. The second data protection principle is parallel to the purpose specification principle and the use limitation principle. The third data protection principle is parallel to the principles of proportionality and data minimization. The fourth data protection principle is parallel to the access/participation principle and the integrity principle. The fifth data protection principle is parallel to the use limitation principle. The sixth data protection principle is parallel to the principles of notice/awareness and consent/choice. The seventh data protection principle is parallel to the principle of security/integrity.

Part V of the DPA implements the principle of enforcement/redress through the establishment of a Data Protection (Information) Commissioner with the authority to intervene in suspected breaches of the DPA by data controllers and issue enforcement notices requiring rectification. The Data Protection Commissioner may also be granted

[376] *Ibid.*

[377] Data Protection Act 1998, Schedule 1, Part I.

a warrant from a circuit judge to enter and inspect the premises of a data controller. The DPA also provides for prosecutions of persons suspected of violating the provisions of the DPA and, if found guilty, those persons are subject to penalties.

Personal data is defined in Article 2 (a) of Directive 95/46/EC as:

> any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

The definition of personal data in the DPA is different in wording and format from Directive 95/46/EC. Part 1, Section 1(1) of the DPA defines personal data as:

> data which relate to a living individual who can be identified –
> (a) from those data, or
> (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Moreover, in order to determine if data is 'personal', any feasibly possible means to link the data with data relating to an identifiable individual should be taken into account. As Recital 26 of EU Directive 95/46/EC states:

> to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person.

However, as the Article 29 Working Party argues, Recital 26

> means that a mere hypothetical possibility to single out the individual is not enough to consider the person as "identifiable". If, taking into account "*all the means likely reasonably to be used by the controller or any other person*", that possibility does not exist or is negligible, the person should not be

> considered as "identifiable", and the information would not be considered as "personal data".[378]

But, as the Article 29 Working Party further adds, this should particularly "take into account all the factors at stake", including the cost of conducting the identification, the intended purpose and the advantage expected by the controller, and should consider "the state of the art in technology at the time of the processing and the possibilities for development during the period for which the data will be processed".[379]

The UK's Information Commissioner's Office (ICO) is responsible for ensuring that all organizations comply with the obligations of the DPA and has, to a certain extent, the enforcement powers to do so. CCTV operators (i.e. data controllers) must use CCTV systems in accordance with the DPA's data protection principles (where relevant) and the DPA also requires CCTV operators to register with the ICO (Taylor, 2002a). In accordance with Section 51 (3)(b) of the DPA (and Article 27 of Directive 95/46/EC), the ICO also issued the 'CCTV code of practice' to help operators of CCTV surveillance systems to comply with the DPA (where relevant). The CCTV code of practice was updated in July 2000 and again in January 2008.

The UK is a party to the ECHR. The Human Rights Act 1998 (HRA) incorporated the ECHR into UK domestic law, requiring domestic courts to take into consideration the decisions of the ECtHR and requiring all domestic legislation to be interpreted in a way consistent with the ECHR. But, the HRA does not mandate that UK domestic courts must observe ECtHR jurisprudence.[380]

Article 8(1) of the ECHR states:

> Everyone has the right to respect for his private and family life, his home and his correspondence.

It is generally accepted that the right to privacy is not absolute and may be infringed under certain circumstances. Accordingly, Article 8(2) states:

---

378 Article 29 Working Party, Opinion 4/2007 on the concept of personal data (WP 136), p. 15.

379 *Ibid*.

380 For further discussion, see Taylor, Nick. *State Surveillance and the Right to Privacy* (Surveillance & Society 1, 2002a), pp. 66-85.

> There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

With the entry into force of the Treaty of Lisbon in 2009,[381] the Charter of Fundamental Rights of the European Union is equally applicable within UK law and is enforceable within UK domestic courts. Article 7 of the Charter provides for the right to privacy, and Article 8 explicitly stipulates:

1. Everyone has the right to the protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

The Treaty of Lisbon also elevates the right to the protection of personal data in EU law through the adoption of a specific article on the right.[382] Article 16 B (para. 1) of the Treaty on the Functioning of the European Union (TFEU)[383] affirms, "Everyone has the right to the protection of personal data concerning them". Article 16 B (para. 2) grants the EU (i.e. the European Commission, European Parliament and the Council) the power or legal basis to legislate and adopt data protection rules applicable to all sectors, including in the area of freedom, justice and security, and therefore alters the limitations of Article 3 of Directive 95/46/EC.[384]

---

[381] Treaty of Lisbon amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007 (OJ C 306, 17.12.2007).

[382] For further discussion, see Cannataci, Joseph A. *Lex Personalitatis: Personality, Law and Technology in the 21st Century* (Acta Universitatis Lucian Blaga 219, 2008).

[383] see Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union (OJ C 83, 30.3.2010)

[384] see Com (2007) 87 final, Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive.

Accordingly, the EC has adopted a draft proposal for a Directive on the protection of individuals with regard to the processing of personal data for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal offences.[385] The proposal builds on Directive 95/46/EC and the Council Framework Decision 2008/977/JHA (hereinafter: CFD 2008/977/JHA),[386] which addresses the protection of personal data processed by law enforcement authorities in criminal matters and complements Directive 95/46/EC. The United Kingdom also takes part in CFD 2008/977/JHA, in accordance with Article 5 of the Protocol integrating the Schengen acquis into the framework of the European Union.[387]

Purportedly, CCTV surveillance systems are being deployed in the UK to prevent crime (Taylor, 2002a, p. 79). However, while an interference with the right to privacy is permitted, any interference must demonstrate both that it is necessary to fulfill a legitimate aim and is proportionate to fulfilling that aim.[388] Some authors question, for example, whether or not the widespread use of CCTV surveillance systems in public spaces is a proportionate response for preventing crime (see, e.g. Taylor, 2002a, p. 80). In addition, any interference with the right to privacy by public authorities must be "in accordance with the law", and the consequences of the law must be foreseeable.[389]

Certain interpretations of Article 8 of the ECHR finely suggest the notion that even activities or incidents involving identifiable individuals that occur in public and are permanently or systematically recorded may be considered private and may thus engage the right to privacy, albeit balanced with the interests of national or public security. The ECtHR has recognized the possibility of the blurring of the public and private spheres. For instance, in *P.G. and J.H. v. the United Kingdom*, the ECtHR held that there "a zone of interaction of a person with others, even in a public context, which may fall within the scope of "private life"'.[390] The ECtHR also held that:

385 see Proposal for a Directive of the European Parliament and of the Council on the protection of Individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final, Brussels, 25.1.2012 (Article 1).

386 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (30.12.2008).

387 *Ibid*., recital 43

388 see Charter of Fundamental Rights of the European Union, Article 52(1).

389 see, e.g., *Kopp v. Switzerland*, Application No. 23224/94, Judgment of 25 March 1998.

390 *P.G. and J.H. v. the United Kingdom*, Application No. 44787/98, Judgment of 25 September 2001, para. 56.

> A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character. Private-life considerations may arise, however, once any systematic or permanent record comes into existence of such material from the public domain. It is for this reason that files gathered by security services on a particular individual fall within the scope of Article 8, even where the information has not been gathered by any intrusive or covert method.[391]

In *Peck v. the United Kingdom*, the ECtHR judged that the publication or general disclosure for broadcasting purposes of images of identifiable individuals obtained by public space CCTV cameras constitutes an intrusion of the right to privacy enshrined in Article 8 of the ECHR. The ECtHR stated:

> Private life is a broad term not susceptible to exhaustive definition. The court has already held that elements such as gender identification, name, sexual orientation and sexual life are important elements of the personal sphere protected by Art.8. The Article also protects a right to identity and personal development, and the right to establish and develop relationships with other human beings and the outside world and it may include activities of a professional or business nature. There is, therefore, a zone of interaction of a person with others, <u>even in a public context</u>, which may fall within the scope of 'private life' (emphasis added).[392]

Furthermore, in *Niemietz v. Germany*, the ECtHR judged:

> it would be too restrictive to limit the notion to an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings.[393]

391 *Ibid.*, para. 57.

392 *Peck v. the United Kingdom*, Application No. 44647/98, Judgment of 28 January 2003, para. 57.

393 *Niemietz v. Germany*, Application No. 13710/88, Judgment of 16 December 1992, para. 29.

As Harris et al. argue, "the expanding understanding of private life set out in the *Niemietz* case indicates that a formal public/private distinction about the nature of the location will not always be decisive" (1995, p. 309).[394]

An infringement of privacy can be associated with the infringement of other rights. The ECtHR in *Segerstedt-Wiberg and others v. Sweden* recognized that an unjustified violation of the right to privacy could also be associated with a violation of the rights to freedom of expression and freedom of (peaceful) assembly, enshrined in Articles 10 and 11 of the ECHR respectively. The ECtHR affirmed that

> the storage of personal data related to political opinion, affiliations and activities that is deemed unjustified for the purposes of Article 8 § 2 *ipso facto* constitutes an unjustified interference with the rights protected by Articles 10 and 11.[395]

Therefore, in order to determine the extent to which public surveillance activities may breach Article 8 of the ECHR, one must carefully consider the purposes and basis for the surveillance and the subsequent use and/or disclosure of the audio and video/image data collected.

Finally, it is also important to note here, however, that the DPA and Directive 95/46/EC apply to all data controllers, while the HRA and ECHR only apply to public authorities. Nonetheless, in accordance with Section 3 of the HRA, the DPA must still be legally interpreted in a way consistent with the ECHR.

---

394 For further discussion, see Taylor, Nick. *State Surveillance and the Right to Privacy* (Surveillance & Society 1, 2002a), pp. 66-85.

395 *Segerstedt-Wiberg and others v. Sweden*, Application No. 62332/00, Judgment of 6 June 2006, para. 107.

6.7.1 CCTV microphones

Based on the privacy/data protection principles, the purpose(s) of any CCTV surveillance system should be specified beforehand and the processing of the images (of identifiable persons), or any other (personal) information obtained via CCTV surveillance systems, must be compatible with the lawful and specified purposes. The use of CCTV surveillance systems must only correspond to achieving these specified purposes. The data collected should also not be retained for longer than is necessary to achieve the specified purposes. In addition, based on the privacy/data protection principles, signs must be displayed to clearly inform the public that they are entering an area monitored by CCTV cameras.

Both audio and image data may qualify as personal data.[396] Appropriately, the former Information Commissioner Richard Thomas declared that sound recorded by CCTV cameras would be treated under UK law in the same way as CCTV footage.[397]

Up until January 2008, the CCTV code of practice, however, did cover sound recording capabilities of CCTV cameras. The updated CCTV code of practice issued in January 2008 addresses the concern of CCTV microphones, but does not forbid their use, as somewhat misleadingly reported by *The Telegraph*.[398] Instead, the CCTV code of practice (2008) advises against recording conversations unless in exceptional circumstances and with the presence of signs. The CCTV code of practice (2008) states:

> CCTV must not be used to record conversations between members of the public as this is highly intrusive and unlikely to be justified. You should choose a system without this facility if possible. If your system comes equipped with a sound recording facility then you should turn this off or disable it in some other way. There are limited circumstances in which audio recording may be justified, subject to sufficient safeguards. These could include: Audio based alert systems (such as those triggered by changes in noise patterns such as sudden shouting). Conversations must not be recorded, and operators should not listen in.[399]

---

396 see Directive 95/46/EC, Recital 14.

397 "Word on the street ... they're listening" (Sunday Times, 26 November 2006), available at: http://www.timesonline.co.uk/tol/news/uk/article650166.ece

398 Hennessy, Patrick. "CCTV camera microphones to be axed" (Telegraph, 28 January 2008), available at: http://www.telegraph.co.uk/news/uknews/1576686/CCTV-camera-microphones-to-be-axed.html#continue

399 CCTV code of practice 2008, p. 10.

Any automated decision, using intelligent software, pertaining to the audio data recorded from the CCTV microphones, would fall under Article 7 of the CFD 2008/977/JHA and would thus be subject to its safeguards.

6.7.2 CCTV loudspeakers

While the CCTV code of practice addresses the use of CCTV loudspeakers, it is difficult to determine the relevant binding statutory laws and case law that pertain to CCTV loudspeakers. The CCTV code of practice exclusively addresses CCTV loudspeakers with the following statement:

> The use of audio to broadcast messages to those under surveillance should be restricted to messages directly related to the purpose for which the system was established.[400]

CCTV loudspeakers are being used to curtail anti-social behaviour, which is rather broadly defined by the Crime and Disorder Act 1998 as acting

> in a manner that caused or was likely to cause harassment, alarm or distress to one or more persons not of the same household as himself.[401]

Anti-social behaviour may include the following acts, just to name a few: vandalism, graffiti, indecent exposure, inappropriate sexual conduct in public, soliciting, illegal parking, fly tipping,[402] public drunken behaviour, and urinating or defecating in public.

---

[400] *Ibid.*, p. 11.

[401] Section 1, para. 1 (a).

[402] Fly tipping is a form of littering that involves dumping large objects or large quantities of material.

6.8 DEFICIENCIES AND DILEMMAS OF THE UK LEGAL FRAMEWORK

Based on the principles of privacy and the criteria of adequacy, as outlined in Chapter 3, an assessment of the UK legal framework reveals significant legal dilemmas and deficiencies, with regards to the deployment and use of public space CCTV microphones and loudspeakers.

6.8.1 CCTV microphones

The DPA certainly incorporates the data protection principles and fully transposes Directive 95/46/EC into UK law. Although the data protection legislation was not originally foreseen to cover CCTV surveillance, Directive 95/46/EC indeed covers both audio and video surveillance, as recognized by the Article 29 Working Party,[403] and in accordance with Recital 14 of Directive 95/46/EC. Still, the DPA or Directive 95/46/EC does not provide a comprehensive legal framework for regulating CCTV surveillance systems, in particular concerning the latest enhancements to public CCTV surveillance capabilities. Besides, as the EC has acknowledged, "[t]he combination of sound and image data with automatic recognition imposes particular care when applying the principles of the Directive".[404] Moreover, the DPA, for the most part, regulates the processing, retention and dissemination of personal data, which may or may not include the audio/video data collected through public space CCTV surveillance systems, but does not actually regulate the deployment of public space CCTV systems nor does it regulate their general use when no audio/video data is stored. This could mean that, even if the DPA regulates the subsequent use of the audio data collected and stored via CCTV microphones, the DPA may not necessarily regulate the use of CCTV microphones to simply listen in to conversations occurring out in public.

All the same, Directive 95/46/EC does not apply to the processing of personal data concerning public security, defence, state security or the activities of the State in areas of criminal law. In particular, Article 3 of Directive 95/46/EC excludes "activities of the State in areas of criminal law" and "operations concerning public security". Moreover, the audio data collected through CCTV microphones is exempt from the first data protection principle of the DPA, since the UK Government is arguably deploying and using

---

403 see Article 29 Working Party, Opinion 4/2004 on the Processing of Personal Data by means of Video Surveillance (WP 89).

404 Com (2007) 87 final, Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, p. 7.

public CCTV microphones to prevent or detect crime.[405] This exemption is equally in line with Article 13 of Directive 95/46/EC.

Again, Article 16 B (para. 2) of the TFEU creates a legal basis for the EU to legislate and adopt instruments applicable to all sectors, including in the area of freedom, justice and security, and therefore also alters the limitations of Article 3 of Directive 95/46/EC.[406] But, in accordance with Article 6a of Protocol No 21 of the Treaty of Lisbon, the UK is not bound by the rules laid down on the basis of Article 16 when carrying out activities which fall within the scope of Chapter 4 or Chapter 5 of Title V of Part Three of the Lisbon Treaty, which deal with criminal matters. In addition, while the Charter of Fundamental Rights of the European Union, including Articles 7 and 8, also applies to the UK (as an EU Member State), in accordance with Article 51, the Charter is not applicable to activities, which are considered a domestic matter outside the scope of EU law.

While CFD 2008/977/JHA aims to protect individuals with regards to processing of their personal data for law enforcement purposes, the scope of the Framework Decision has a limited scope of application, since it only applies to the cross-border data processing of law enforcement agencies and not national/domestic activities.[407] Furthermore, as Cannataci (2010) notably points out, CFD 2008/977/JHA does not provide any concrete details on how to uphold the rights of data subjects affected by 'smart surveillance' or MIMSI surveillance systems.

The fact that Article 3 of Directive 95/46/EC excludes "activities of the State in areas of criminal law" and "operations concerning public security" and the fact that the scope of CFD 2008/977/JHA is limited to cross-border data processing compelled

[405] Data Protection Act 1998, s. 29 (1) (a).

[406] For further information, see Com (2007) 87 final, Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive. (Hence, the reason for the emergence of the Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final, Brussels, 25.1.2012.

[407] see Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (30.12.2008), recital 3. For further discussion, see Cannataci (2010).

the EC to propose a new Directive on the protection of individuals with regard to the processing of personal data for law enforcement purposes.[408]

With regards to the general use of CCTV microphones, the legal framework additionally does not fulfill the ***principles of use limitation*** and ***purpose specification***. To begin with, the judgment adopted by the Court of Appeal in *Durant v. Financial Services Authority*[409] narrowed the meaning of 'personal data' in the UK. For data to be "personal" the concerned individual needs to be the "focus" and the data needs to be intended to provide specific intelligence of a "biographical" nature about a particular person.[410] As Rempell (2006) notably argues, this narrowed definition of personal data, which was accomplished by narrowing the meaning of the words "relate to" within the definition, is flawed (2006, p. 823) and is against the proper intentions of the drafters of Directive 95/46/EC for a broader definition (2006, pp. 825-26). As Rempell concludes in his analysis of the judgment, the problem is not necessarily with the content of the DPA, but rather the Court of Appeal's decision, which seriously deviates from Directive 95/46/EC (2006, p. 840). In direct response to the judgment, the ICO was forced to issue corresponding guidance on the definition of what amounts to personal data.[411]

The consequences of *Durant v. Financial Services Authority* went beyond data held by the Federal Services Authority (FSA) and, as widely recognized, directly affected the data captured via public space CCTV cameras (Rempell, 2006). With regards to the images generated by public space CCTV cameras, the narrowing of the definition of personal data essentially meant that if only a general scene is recorded with no focus on any particular individual's activities, these images are not covered by the DPA, as they are no longer regarded as personal data (Rempell, 2006). Therefore, in actuality the DPA does not apply to a large part of the data captured by public CCTV cameras.

---

408 see Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final, Brussels, 25.1.2012.

409 *Michael John Durant v. Financial Services Authority* [2003] EWCA (Civ) 1746. Durant made a request under Part II, Section 7 of the Data Protection Act 1998 to obtain 'personal data' about him which was held by the Financial Services Authority (FSA). The FSA refused to provide all the data requested by Durant, arguing that not all of it constituted personal data, and emphasized that the definition of the words "relate to" in the DPA's definition of personal data meant "have reference to, concern" instead of "have some connection with, connected to" (para. 25). The Court of Appeal agreed with the FSA.

410 *Ibid.*, para. 28.

411 "*The Durant case and its impact on the interpretation of the Data Protection Act 1998'", Information Commissioner's Office, 2 February 2004.*

Equally, likely for the same reason, the ICO determined that Google Street View does not breach the DPA.[412]

Following pressure from the EC[413] and the threat that the EC could begin infringement procedures against the UK for the unacceptable or objectionable implementation of Directive 95/46/EC, and the adoption by the Article 29 Working Party of a much broader interpretation of personal data,[414] the ICO issued once again revised guidance, titled "Data Protection Technical Guidance – determining what is personal", which stretched, to a certain extent, the narrow definition of personal data in the UK. But, the judgment of the Court of Appeal in *Durant v. Financial Services Authority* is legally superior to the guidance of the ICO. Nevertheless, as a result of the Charter of Fundamental Rights of the European Union and the entry into force of the Treaty of Lisbon, both the European Commission and UK citizens could potentially further challenge the UK's implementation of the DPA (i.e. Directive 95/46/EC).

Overall, the situation represents an example of the non-uniform implementation and interpretation of the provisions of Directive 95/46/EC by EU Member States (Rempell, 2006), and the UK's common practice of moving beyond the limits of the "margin of maneuver" as permitted by Recital 9 of Directive 95/46/EC.[415]

Applying the same rationale of *Durant v. Financial Services Authority* to audio recorded by CCTV microphones, general sound recorded in public is not considered personal data and therefore is not covered by the DPA, since it is not focused on any particular individual. With additional technology, however, the background noise can be filtered out using inverse phasing, which cancels out unwanted noise, to discern private conversations concerning particular individuals. Therefore, general sound recorded in public at the point of collection might not be considered personal data, but may later be converted, with little effort, into personally identifiable information and, in accordance with Recital 26 of Directive 95/46/EC, constitute personal data.

---

[412] Information Commissioner's Office, Press Release, "Common sense on Street View must prevail, says the ICO", available at: http://www.ico.gov.uk/upload/documents/pressreleases/2009/google_streetview_220409_v2.pdf

[413] see "European Commission suggests UK's Data Protection Act is deficient" (OUT-LAW News, 15 July 2004), available at: www.out-law.com/page-4717

[414] see Article 29 Working Party, Opinion 4/2007 on the concept of personal data (WP 136).

[415] Hence, the reason why the EC has proposed to replace Directive 95/46/EC with a Regulation, in order to eliminate the existing fragmentation and to ensure the uniform and effective implementation of the data protection rules within every EU Member State. For further discussion, see COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, Safeguarding Privacy in a Connected World, A European Data Protection Framework for the 21st Century, COM(2012) 9 final, Brussels, 25.1.2012.

However, even if general sound recorded in public and stored on databases could be considered personal data, or construed as such, and thus protected by the DPA, the act of recording sound out in public is not prohibited. In essence, only what is done with that stored audio data afterwards is regulated.

Nevertheless, audio data collected from public CCTV microphones is wrongfully being equated with video data collected from public CCTV cameras. Audio data, even recorded in public, can be considerably more 'sensitive', since it may record private conversations and thus the political opinions and religious beliefs of individuals – information which video data normally cannot discover, unless the messages/words are both written down, for example on a sign or t-shirt, and are discernible via the CCTV cameras.

With further sophistication, CCTV microphones can also potentially lead to the greater identification and tracking of individuals in public. Software can identify an individual by comparing their voice with voice-prints[416] stored in a database. According to the Police IT Organization (PITO), voice is an additional mode of identification that is already being considered for inclusion into IDENT1,[417] the UK central national database for storing biometric information.[418] The legal framework does not necessarily prevent the use of CCTV microphones for this purpose.

Furthermore, the CCTV code of practice (2008) addresses CCTV microphones, but it is not binding law in itself and does not offer any actionable rights for citizens. Nevertheless, the CCTV code of practice (2008) only briefly deals with the issues surrounding CCTV microphones, lacks specificity and leaves open several legal loopholes. Although the CCTV code of practice (2008) states, "CCTV must not be used to record conversations between members of the public as this is highly intrusive and unlikely to be justified",[419] it is unclear what is the actual legal basis of this declaration. Nor is it clear whether this includes conversations occurring in public places, particularly if people are aware that microphones are being overtly fitted to public space CCTV cameras.

Supporters in favor of public CCTV microphones could argue that if a person does not want to be heard or recorded, he/she can choose not to speak when out in public or at least not about 'sensitive' topics, such as religion or politics. Moreover, it can be further argued that the presence of any CCTV surveillance system is merely comparable to

---

[416] A voice-print is data representing patterns in a digital recording of an individual's voice.

[417] PART 1: Identification Roadmap 2005 – 2020, Biometrics Technology Roadmap for Person Identification within the Police Service, Police IT Organization, p. 4.

[418] However, the Identity Documents Act 2010 recently repealed the Identity Cards Act 2006, which permitted the recording of any type of biometric information for the National Identity Register (NIR).

[419] CCTV code of practice 2008, p. 10.

the presence of an individual observer, such as a security guard. As the ECtHR in *P.G. and J.H. v. the United Kingdom* judged:

> A person who walks down the street will, inevitably, be visible to any member of the public who is also present. Monitoring by technological means of the same public scene (for example, a security guard viewing through closed-circuit television) is of a similar character.[420]

Therefore, since CCTV cameras installed in public places are already legitimately considered as the eyes of security guards or law enforcement officers/agents, microphones could legitimately be considered as their ears.

While covertly recording private conversations is regulated and is often considered eavesdropping, like video surveillance, it is only prohibited, without due authorization, in areas where privacy can reasonably be expected. Although Moreham (2006) is indeed correct in arguing that a person would have a reasonable expectation that another person, for instance, is not recording their conversations with a shotgun microphone, however, any expectation of privacy of conversations out in public straightaway vanishes with the positioning of signs or notices warning that public space CCTV cameras fitted with microphones are present. Accordingly, the notices would cause the audio recording to be conducted overtly, as opposed to covertly. Continuing to speak out in public, while knowing or having been given notice that microphones are present, could be legally considered as implicit consent to be recorded. Audio recording is not considered eavesdropping when consent is given and/or the persons concerned have been informed.

Moreover, the Regulation of Investigatory Powers Act 2000 (RIPA) does not cover the overt, general use of public CCTV microphones, in accordance with paragraph 1.4 of the Covert Surveillance Code of Practice, unless specifically used for targeted/directed surveillance for specific investigations. The covert use of CCTV microphones in public spaces for targeted/directed surveillance by police or local authorities is also still lawful, albeit subject to certain safeguards of RIPA. Furthermore, as Donohue (2006) asserts, there is no legitimate expectation of privacy of illegitimate activities in public places, pointing out that the ECtHR previously judged that there is no legal authority in the UK for the judicial regulation of police placing a microphone on the outside of a building (Donohue, 2006).[421]

---

420 *P.G. and J.H. v. the United Kingdom*, Application no. 44787/98, Judgment of 25 September 2001, para. 57.

421 see *Khan v. United Kingdom*, Application no. 35394/97, Judgment of 12 May 2000.

Although under the latest CCTV code of practice (2008), CCTV surveillance systems are supposed to not be used for recording private conversations, the law arguably permits the random or general recording of the public at large, as long as it is done so in a public place and especially if the public is informed that CCTV microphones are present. The general observation or surveillance of public places is lawful, while conversations knowingly exposed in public are not protected. As Taylor points out, although the influence of Article 8 of the ECHR "has not yet been fully realised in the area of [overt] public space surveillance" (2002a, p. 73), "to find that CCTV surveillance in public spaces is a breach of privacy per se would be to broaden Article 8 in a way that, it appears, the European Court [ECtHR] is not prepared to do" (2002a, p. 76). Furthermore, as Victoria Williams argues, while Article 8 of the ECHR and ECtHR jurisprudence may recognize a legal basis for privacy in public spaces, the conventional notions of privacy do not translate well in public settings.[422]

The legal framework is equally ***ambiguous and vague***. For instance, the language of the CCTV code of practice (2008) is particularly problematic. It permits "limited circumstances in which audio recording may be justified, subject to sufficient safeguards", such as "audio based alert systems triggered by changes in noise patterns such as sudden shouting".[423] However, it does not explain what are these "limited circumstances" and "sufficient safeguards".

CCTV microphones can be triggered on the basis of decibel level or sound intensity and the speed at which words are spoken. With artificial intelligence (AI) technology,[424] the microphones can also be triggered by certain key words, such as expletive words considered aggressive.

Nevertheless, "sudden shouting" should not be enough to warrant the activation of the recording of CCTV microphones. This would permit the recording of a brief argument or heated debate between two or more people, which cannot justifiably be considered necessary for preventing or detecting crime. Moreover, the CCTV code of practice uses the words "*such as* sudden shouting" (emphasis added), which indicates that other criteria or circumstances are permitted to trigger CCTV microphones to begin recording.

---

422 see, for further discussion, the Memorandum by Victoria Williams for the House of Lords Constitution Committee inquiry into the impact of surveillance and data collection upon the privacy of citizens, available at: http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/8051402.htm
Victoria Williams is the author of the *Surveillance and Intelligence Law Handbook* (Oxford University Press, 2006).

423 CCTV code of practice 2008, p. 10.

424 Artificial-intelligence is defined as "the art of creating machines that perform functions that require intelligence when performed by people". Kurzweil, Ray. *The age of intelligent machines* (MIT Press, 1990), p. 14.

The triggering of CCTV microphones to begin recording once a certain sound intensity[425] is reached is both unwarranted and impractical. A normal spoken conversation, for example at 60 decibels (dB) or more, can have about the same sound intensity level as ordinary street noise. Traffic, therefore, could trigger recording and in doing so also record normal spoken conversations occurring nearby (see Table 1).[426] Nevertheless, who is to determine with certainty at what intensity in decibels is an exchange between two or more people really an argument or a normal conversation.[427] Such determination could easily vary from culture to culture. Using sound intensity as the basis of triggering CCTV microphones to begin recording will also permit the blanket recording of conversations at noisy locations, such as nightlife areas. While triggering the microphones based on sound intensity is impractical, justifying the recording of conversations out in public because someone uses expletive words or speaks quickly is simply absurd and is against common sense and reason.

Type of Sound	Sound intensity level (dB)
Normal spoken conversation	60
Ordinary street noise	70
Shouting	80
A pneumatic drill in use nearby	110

Table 1: Sound intensity of different types of sounds[428]

425 Sound intensity is the amount of sound energy per unit area. The basic units are either watts/m^2 or watts/cm^2. Sound intensity level is measured in decibels (dB). Decibels measure the ratio of a given sound intensity I to the threshold of hearing. The threshold of hearing is assigned a sound level of 0 decibels, which corresponds to an intensity of 10-12 watts/m^2. A sound that is 10 times more intense (10-11 watts/m^2) is assigned a sound level of 10 dB, and so on. see "sound intensity", Encyclopedia Britannica 2009, Encyclopedia Britannica Online, 11 Nov. 2009, available at: http://www.britannica.com/EBchecked/topic/555343/sound-intensity; "sound", Encyclopedia Britannica 2009, Encyclopedia Britannica Online, 11 Nov. 2009, available at: http://www.britannica.com/EBchecked/topic/555255/sound

426 Note that the distance between the source and the microphones plays a role.

427 Using a Velleman DVM 805 sound level meter, I measured the 'normal' conversation of two colleagues in a quiet office setting for two minutes. The meter was placed at around two meters from the source. While no one was arguing or shouting, the sound levels still reached up to 70 dBA on several occasions. Note: dBA is the meter's use of an "A" filter, which is used to match more precisely what the human ear actually hears by "A-weighting" the decibel measurements.

428 Sources: The Royal National Institute of Deaf People / Encyclopaedia Britannica Online 2009.

Moreover, the law does not place specific limits on the key words the AI software is permitted to be triggered by, which could freely enable the UK Government to use CCTV microphones to monitor conversations out in public, similar to the way conversations over the phone may be monitored.

In sum, there is a lack of harmonized implementation of the Data Protection Directive (Directive 95/46/EC) and consensus on what legally constitutes personal data. The UK legal framework is *ambiguous* and *inconsistent* with regards to both the images and sound captured or recorded via public space CCTV surveillance systems. There is essentially no clear understanding as to the extent to which privacy exists out in public, if it even does exist at all. Moreover, the UK legal framework is not clear on what are the limited circumstances the use of CCTV microphones by law enforcement agencies are justified and the CCTV code of practice (2008) only leaves open more significant legal questions.

6.8.2 CCTV loudspeakers

While the illegitimate and disproportional use of CCTV loudspeakers should be considered an interference with the right to be left alone, it is nonetheless difficult to determine what laws are actually violated. The principles of data protection, for the most part, are not meant in actuality to apply to CCTV loudspeakers, since the loudspeakers themselves do not collect, store or process data. Furthermore, it also difficult to apply Article 8 of the ECHR to CCTV loudspeakers owned and operated by public authorities.

However, the second data protection principle, which is parallel to the *purpose specification principle*, the fifth data protection principle, which is parallel to the *use limitation principle*, and the *principle of proportionality* are still applicable.

The CCTV code of practice (2008) does not at all sufficiently address CCTV loudspeakers, nor fulfill the ***use limitation or purpose specification principles*** and satisfy the required legal characteristics of ***foreseeability*** and ***clarity***. Although the CCTV code of practice (2008) restricts the use of CCTV loudspeakers "to messages directly related to the purpose for which the system was established",[429] it does not define under what circumstances are those purposes legitimate or proportionate, nor the scope of a CCTV control room operator's discretion to use the CCTV loudspeakers, what should and should not be communicated or how and why those messages should be communicated.

[429] CCTV code of practice 2008, p. 7.

There is (or at least was) mounting concern that CCTV surveillance technology is being used for trivial reasons, such as to prevent littering under the "Keep Britain Tidy" campaign, and for other trivial offences, such as public drunkenness, etc. The focus on trivial offences results in more individuals being arrested for such low-level categories of offenses rather than serious crimes (Surette, 2005, p. 155). There is equally growing concern that local governments are excessively taking advantage of the broad powers of the RIPA to carry out surveillance for reasons other than to prevent or detect crime or ensure national/public security. RIPA is rather being used to carry out surveillance for reasons far less important, such as catching people putting out their rubbish too early, failing to clean up their dog's waste or dropping litter, and to investigate noise pollution. According to a freedom of information request made by the *Daily Mail*, more than half of town halls in the last three years have used the powers of RIPA to spy on families suspected of putting their rubbish out on the wrong day. In addition to covertly following the suspected targets, the surveillance tactics have also included putting secret cameras in tin cans and on lampposts.[430] RIPA permits the conduct of surveillance by a variety of public authorities, including town halls and not just the police and intelligence agencies, for reasons of preventing or detecting crime or ensuring national security and to 'protect public health' and the 'economic well-being'.[431] The latter two reasons serve as the potential basis for conducting surveillance for environmental concerns. The problem is, however, that the ambiguous wording of RIPA can justify surveillance operations for a variety of reasons.[432] Surely, there is little concern that the legislation can be used to prevent and punish, for instance, commercial fly tipping. But, abusing the powers of RIPA for trivial reasons is a serious concern. The wider use of CCTV loudspeakers could potentially be further bolstered by the common practice of using CCTV cameras and applying RIPA for trivial reasons.

---

430 Borland, Sophie and James Slack. "March of the dustbin Stasi: Half of councils use anti-terror laws to watch people putting rubbish out on the wrong day" (Daily Mail, 1 November 2008), available at: http://www.dailymail.co.uk/news/article-1082225/March-dustbin-Stasi-Half-councils-use-anti-terror-laws-watch-people-putting-rubbish-wrong-day.html

431 Regulation of Investigatory Powers Act 2000, Part II, Section 28 (3).

432 As a result, proposals to amend RIPA, in order to restrict the ability of local authorities to use CCTV surveillance systems for trivial purposes and to provide for judicial approval in relation to certain authorisations and notices under RIPA, were introduced to Parliament on 11 February 2011 in a bill, titled the "Protection of Freedoms Bill 2010-11".

6.9 RECOMMENDATIONS ON ENHANCING THE UK LEGAL FRAMEWORK

Although, as Taylor (2002, 2002a) argues, UK domestic courts might be in a position to develop the concept of privacy in public spaces, can we really wait for the courts to slowly do so? Public surveillance CCTV systems and enhancements to the technology integrated to these systems demand specific laws from the UK Parliament immediately.

The European Commission for Democracy through Law (Venice Commission) of the Council of Europe published an opinion on video surveillance in public places by public authorities, concluding that

> specific regulations should be enacted at both international and national level in order to cover the specific issue of video surveillance by public authorities of public areas as a limitation of the right to privacy.[433]

Similarly, the Constitution Committee of the UK House of Lords recommended that the UK Government should adopt a statutory regime for the use of CCTV by *both* the public and private sectors, including codes of practice that are legally binding and overseen by the Office of Surveillance Commissioners (OSC) together with the ICO.[434]

Nevertheless, the UK legal framework does not necessarily require a complete overhaul and the DPA presents a basis for public space CCTV operators to work from (see Taylor, 2002a, p. 82-83). While that may be the case, specific rules/regulations are still required to bring clarity to the purpose and scope of CCTV microphones and CCTV loudspeakers. Indeed, as Taylor points out, "[t]here are situations when the state has to intervene in the lives of its citizens, such as to prevent crime, but such intervention must be based on, and restricted by, principled legislation" (*Ibid*., p. 83). A framework or basis by which to distinguish the legitimate and proportional or illegitimate and disproportional use of CCTV microphones and CCTV loudspeakers is required. For the moment, however, regulations on the use and deployment of CCTV microphones and CCTV loudspeakers may not require EU action or intervention, since the deployment of these CCTV enhancements are occurring exclusively in the UK, with the exception of CCTV microphones being tested and deployed in the Netherlands. But,

433 Draft Opinion on Video Surveillance and the Protection of Human Rights, adopted by the Venice Commission at its 70th Plenary Session, Venice, Italy, 16-17 March 2007, para. 81, available at: http://www.venice.coe.int/docs/2007/CDL-AD(2007)014-e.asp

434 Constitution Committee - Second Report, Surveillance: Citizens and the State (Session 2008-09), Chapter 4, para. 219, available at: http://www.parliament.the-stationery-office.com/pa/ld200809/ldselect/ldconst/18/1802.htm

the European Commission and Article 29 Working Party should remain vigilant on any expanded deployment of CCTV microphones and CCTV loudspeakers within Europe.

It is important to point out, on the other hand, that the means to protecting privacy are not just legal-orientated or policy-orientated. Regulating the design and development of CCTV microphones and CCTV loudspeakers can inherently minimize their intrusive capability from the start. Moreover, since there seems to be no clear understanding of the extent to which privacy exists in public, if it even does, or clear way of determining so, there is even more reason to focus on the design, development and deployment of CCTV microphones and CCTV loudspeakers, as opposed to solely on their use. Accordingly, many of the obligations should fall upon the manufacturers of CCTV microphones and loudspeakers, rather than merely on their operators.

In addition, since the effects of both CCTV microphones and CCTV loudspeakers go beyond privacy, their use could pose a serious threat, if left unchecked, to personal freedom and autonomy, freedom of speech and our sense of dignity. The law and technological solutions should therefore also possess the demonstrable ability to preserve both privacy and liberty overall.

6.9.1 CCTV microphones

Indeed, the integration of microphones to CCTV cameras can offer security gains and thus should not be completely outlawed. However, before they are widely deployed, specific regulations must be put into place.

Since it is unclear how and under what circumstances it is lawful or legitimate for law enforcement agencies to use CCTV microphones or whether or not Article 8 of the ECHR (and the DPA) are applicable to the audio data collected, regulations on public space CCTV microphones should explicitly focus on their design, development and deployment for public use, rather than solely on their use, by placing significant limits on the technology itself.

Unlike the SIgard system, or other public CCTV audio surveillance systems, public CCTV microphones, based on the ***principle of proportionality***, must not be capable of recording conversations nor programmed to be triggered by shouting or verbal aggression (or how something is said), since this is not sufficiently justified for the purposes of ensuring public security. Moreover, the temptation for abuse or the propensity towards 'function creep' or 'surveillance creep' is just too great, as we have already seen with the use of CCTV visual surveillance capabilities for voyeurism (Surette, 2005) or 'cheap thrills' in the UK.[435]

The framework or basis by which to distinguish between the legitimate and proportional or illegitimate and disproportional use of CCTV microphones for security purposes should be based on the common understandings of which sounds or noises actually constitute a public danger or security threat and justify their detection and the audio recording of the incident. Therefore, the activation of the recording capabilities of CCTV microphones should be limited to those particular sounds only, thereby guaranteeing the legitimate and proportional use of CCTV microphones. In order to remove all areas of ambiguity, the law should explicitly restrict the activation of the public CCTV microphones to the following set of sounds: gunfire; explosions; breaking glass; car alarms; car crashes; burglar alarms; and screams that contain the specific words "help" or "fire". If and where necessary, the microphones could also detect or recognize these words shouted in other languages. Based on the framework, other sounds and shouted out words might also merit the activation of CCTV microphones. While this list of sounds may not be exhaustive, the delineation of which sounds may activate the CCTV microphones to begin recording must be precise. However, the adding of any additional sounds is up for debate, and security experts, law enforcement agencies and the public at large should be consulted beforehand.

The detection of these diverse, yet very distinct sounds and the two specific words "help" and "fire", shouted at no less than 65 decibels or more, can be achieved with the use of AI software or the incorporation of software agents with reactive abilities.[436] Researchers from the University of Portsmouth are already working to develop AI software that can recognize sounds and words.[437] The incorporation of AI or software agents, however, may also require separate legislation (Schermer, 2007). Moreover, the

[435] see "Peeping tom CCTV workers jailed" (BBC News, 13 January 2006), available at: http://news.bbc.co.uk/1/hi/england/merseyside/4609746.stm

[436] A software agent is any software that exhibits any character commonly associated with agency, such as reactive, proactive, goal orientated, deliberative, communicative and adaptive. Software agents with reactive abilities or characteristics "employ any type and number of sensors to sense its environment. The software can react to sensory input using its actuators" (Schermer, 2007, p. 22).

[437] Thurston, Richard. "CCTV cameras that listen as well as watch" (SC Magazine, 25 June 2008), available at: http://www.scmagazineuk.com/CCTV-cameras-that-listen-as-well-as watch/article/111675/

decisions of a software agent may classify as an "automated individual decision" and, therefore, should set off the safeguards of CFD 2008/977/JHA.[438]

When gunfire, etc. is detected, the microphones can immediately begin to record, calculate the location of the sound source, direct the cameras in that direction and alert the CCTV control room operators, who in turn can alert a police dispatcher to send the closest police officer(s) or unit. Based on the ***purpose specification*** **principle**, however, the audio recording must cease within a definite short period of time after each new event or incident is detected. In addition, based on the ***use limitation principle***, the audio data must only be accessed and used for evidential purposes and, where possible or necessary, any unrelated background sound should be edited out, which could also be helpful for the related criminal investigation and prosecution. Shouting "help" or "fire", in order to intentionally trigger the CCTV cameras without justification, should accordingly be prohibited.

Thus, in line with the ***principle of notice/awareness***, the placement of additional or different notice signs from the ones already available may not necessarily be required, since the CCTV microphones will not record any personal data.

A CCTV system that can only detect the above specific sounds and shouted words, as mandated by law, is the way forward to both enhance public security and guarantee that privacy safeguards are in place and unwavering. Moreover, such a system may require fewer cameras to cover larger areas and thus less recorded visual data of the public space (Kim et al., 2007, p. 389).

6.9.2 CCTV loudspeakers

Even if CCTV loudspeakers do prove to be effective for public safety reasons, they still require the proper checks and balances.

Once again, it is difficult to clearly determine the relevant laws that pertain to CCTV loudspeakers and what laws CCTV loudspeakers violate. Regulations on CCTV loudspeakers should therefore equally focus on their development, manufacture and deployment rather than solely address their use.

---

438 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (30.12.2008), Article 7.
Article 9 of the EC's proposal for a Directive on the protection of individuals with regard to the processing of personal data for law enforcement purposes (COM(2012) 10 final, Brussels, 25.1.2012) prohibits measures based solely on the automated processing of personal data, if not authorised by law and subject to appropriate safeguards (in line with Article 7 of CFD 2008/977/JHA).

Based on the understanding of privacy as the right to be left alone, CCTV loudspeakers should not be capable of being used for disturbing or scolding individuals. The possibility of operators to abuse CCTV loudspeakers by harassing people from afar must be minimized.

Indeed, as Taylor points out, the CCTV operator "phone pest" occurrence,[439] whereby an operator used public pay phones to pester people he could see via CCTV cameras, could not have been prevented by laws that only regulate the collection, use and storage of CCTV images (2002, p. 107). However, regulations concerning the design and development of public space CCTV loudspeakers, in combination with specific rules on their use and specified penalties for misuse, could significantly minimize the chances of this occurring with CCTV loudspeakers.

The use of specific pre-recorded messages and the removal of the ability of CCTV operators to speak directly to the public can automatically limit what operators can communicate via CCTV loudspeakers. The different pre-recorded messages could be activated by entering a designated three-digit number that corresponds with each message onto computer keypads. For example, 146 for "CCTV cameras are monitoring you, please discontinue the graffiti" or 112 for "stay where you are, the police are on their way". CCTV loudspeakers should only be capable of delivering these pre-recorded messages at a certain volume and should not use the voice of children to leverage their so-called "pester power" nor the voice of celebrities to leverage their influence, but rather a generic male or female voice.

Some might argue that the use of pre-recorded messages will make it difficult to deliver more specific or detailed messages, since they are fixed. However, surely one of the hundred or so different pre-recorded messages that can be stored will be capable of getting the appropriate point across to the concerned individual(s). Others might also argue that discovering the correct three-digit number to enter in order to deliver the appropriate pre-recorded message will take longer or prove more difficult than speaking directly. But, an electronic list of the available pre-recorded messages can be easily displayed on a monitor. Moreover, trained and experienced operators will begin to memorize a number of different three-digit numbers and their corresponding pre-recorded messages, which might in fact enable operators to communicate with targeted individuals quicker, easier and more effective than having to do so by spoken words. Pre-recorded messages, rather than speaking directly to perpetrators, might also enhance compliance and reduce the provoking of rebellious acts in response.

---

439 see "Phone Pest picked targets on security video" (The Telegraph, 7 June 1996), available at: www.telegraph.co.uk/htmlContent.jhtml?html=/archive/1996/11/27/ntel27.html

Even pre-recorded messages can be illegitimately, inappropriately and/or disproportionately used, resulting in the unnecessary cause of harm to a person's dignity or individual liberties and the unnecessary disturbance of the public peace. The framework by which to distinguish if the use of CCTV loudspeakers is legitimate and proportional should be based on whether or not their use serves the purpose of preventing, deterring or discontinuing an anti-social act that threatens public security and/or well-being.

The pre-recorded messages used to prevent, deter or discontinue an anti-social act must be used in accordance with the Anti-Social Behaviour Act 2003 and not for trivial reasons that do not threaten public security and/or well-being. For instance, littering, such as dropping a chewing gum wrapper or putting out a cigarette on the sidewalk, does not justify the use of CCTV loudspeakers. Only more serious forms of littering and hazards to the environment, such as fly tipping, justify the use of CCTV loudspeakers. More to the point, the law should also further clarify that the powers of RIPA should not be used for trivial reasons.[440] Besides, the use of CCTV loudspeakers for trivial reasons would likely lead to rebellious acts and depreciating levels of compliance.

Still, the automatic limitation on what can be communicated using CCTV loudspeakers via pre-recorded messages already provides the means to better preserve the legitimate use of CCTV loudspeakers and prevent harm to a person's dignity and personal autonomy.

In the end, it is the public CCTV operators who have to make the decision whether or not to use the loudspeakers. Keeping track of the number of times the CCTV loudspeakers are used will help to ensure they are being used legitimately and proportionally, and not for 'cheap thrills' or on grounds of discrimination. Since the pre-recorded messages are activated by entering numbers into computer keypads, tracking the use of CCTV loudspeakers can be done automatically. This will also permit an accurate and easier evaluation on their impact in each specific area.

Taylor argues that "[i]f Article 8 [of the ECHR] were to apply to public visual surveillance systems it would at least ensure a debate about whether or not CCTV surveillance could be justified in an individual situation, or whether other methods of crime prevention might be equally, or more, successful with less intrusion" (2002a, p. 81). Taylor goes on to write that "[i]f Article 8 were engaged the issue of proportionality would require that the least obtrusive means necessary should be undertaken, thus

[440] Proposals to amend RIPA, in order to restrict the ability of local authorities to use CCTV surveillance systems for trivial purposes and to provide for judicial approval in relation to certain authorisations and notices under RIPA, were introduced to Parliament on 11 February 2011 in a bill, titled the "Protection of Freedoms Bill 2010-11". The bill also calls for the appointment of a Surveillance Camera Commissioner and introduces a code of practice for surveillance camera systems. As of October 2011, the bill has only just entered into the report stage in the House of Commons.

not barring surveillance, but ensuring it is appropriate and justifiable" (*Ibid*., p. 81-82). Accordingly, this would call for the deployment of CCTV loudspeakers to be restricted to certain areas of public space, which have credibly been identified as 'hotspots' or high-risk areas of anti-social behaviour and where an evaluation has determined that the CCTV loudspeakers would be the appropriate and effective solution to the problem. This will better ensure that CCTV loudspeakers are proportionally deployed and that their deployment and use is based on legitimate aims, in accordance with the law and the ***principle of purpose specification*** and ***principle of proportionality***. In addition, before a decision is taken by local authorities to deploy CCTV loudspeakers anywhere, there should be an open dialogue with the surrounding neighborhood or the public directly affected.

The well thought-out deployment of CCTV loudspeakers will also help ensure the noise generated by the loudspeakers does not unnecessarily disturb those nearby. CCTV loudspeakers should equally be banned from being deployed nearby medical facilities so as to not disturb patients. Perhaps, the use of CCTV loudspeakers should also be prohibited during certain times of the day, unless in exceptional circumstances that merit their use, such as to prevent serious crimes, rather than low-level anti-social behaviour.

With "single wire digital transmission" technology, for example, thousands of CCTV loudspeakers could potentially be operated individually or in groups from a single location hundreds of kilometers from where they are located. However, in order to check the concentration of power, the law should prohibit the centralization of the ability to operate that many CCTV loudspeakers from a single control room.

With more advanced technology, such as HyperSonic Sound (HSS),[441] it may also be possible to deliver the pre-recorded messages in a way only audible to the targeted individual. The basis of excluding CCTV loudspeakers from certain public areas in order to ensure the sound does not unnecessarily disturb others may, as a result, no longer be compelling. Still, the use of HSS in CCTV loudspeakers should be banned in order to ensure 'mental privacy', which also requires separate legislation in itself.

CCTV loudspeakers can be used as a form of verbal warning or reprimand for juveniles or means to convey informal punishments. Therefore, if CCTV loudspeakers are to be the "voice of authority",[442] then only publicly authorized public authorities should

---

441 HyperSonic Sound technology, developed by American Technology Corporation, provides the ability to direct sound to a specific area or target, similar to light, using ultrasonic sound energy. American Technology Corporation, available at: http://www.atcsd.com/site/content/view/34/47/

442 "Talking CCTV brings voice of authority to streets", Home Office, 4 April 2007, available at: http://www.homeoffice.gov.uk/about-us/news/talking-cctv

be allowed to use them. Furthermore, the integration of loudspeakers must be restricted to publicly owned and managed surveillance CCTV systems.

The law needs to specify the consequences of ignoring verbal warnings communicated via CCTV loudspeakers for anti-social behaviour. After the first verbal warning, if the perpetrator does not comply, then a second verbal warning should follow. If the perpetrator still does not comply, then a police officer should be dispatched, when necessary, to resolve the issue or penalize that person, in accordance with the law.[443] Under certain circumstances, fines and/or ASBOs could be issued after failing to comply with the second warning. If the person runs from the scene, the perpetrator could potentially be identified, with the enhancement of CCTV image quality, addition of face recognition technology[444] and linkage to the NIR. The verbal warning or reprimand can then be registered in the record of the person concerned.

Failure to comply with verbal warnings from CCTV loudspeakers to refrain from anti-social behaviour does not immediately merit the use of non-lethal force deterrence technology, also known as less-than-lethal force or compliance weapons. However, the integration of non-lethal deterrence technology to public space CCTV cameras, such as the scheme developed by ICx Imaging Systems, which consists of a high-powered strobe light to temporarily disorientate perpetrators,[445] or LRADs could be legitimate if used to bring to an end violent or dangerous acts alone and subject to specific rules.[446] The use of less-than-lethal force simply for crowd control should be considered illegitimate.

Still, CCTV control room operators should receive additional special training, in coordination with the Home Office, in order to be allowed to operate the loudspeakers. Training should ensure that the operators are better equipped to base their decision on using CCTV loudspeakers in a standardized and objective manner and in accordance with the relevant privacy principles and framework of proportionality and necessity, as far as humanly possible, and with a sound knowledge and understanding of the special circumstances in their area.

---

443 Crime and Disorder Act 1998; Anti-Social Behaviour Act 2003.

444 "Better CCTV needed for ID" (BBC News, 11 May 2006), available at: http://news.bbc.co.uk/2/hi/uk_news/politics/4761519.stm

445 ICx Technologies, Inc., http://www.icxt.com/products/icx-surveillance/thermal-imaging/illuminator/

446 LRADs are already being deployed in the US by police for crowd control purposes and this recent development has rightfully caused an outrage. see "Sheriff's Department Responds To Sonic Device Outrage" (10news.com, 15 September 2009), available at: http://www.10news.com/news/20931535/detail.html
LRADs were most recently deployed and used by police for protests during G20 Pittsburgh Summit.

CCTV loudspeakers can also be used alongside 'intelligent' CCTV cameras. With the use of software agents, the pre-recorded messages could instead be activated exclusive of human involvement. Software agents with the ability to deliberate extensively before reacting (Schermer, 2007, p. 22) could determine when an anti-social act is being committed and then broadcast the relevant pre-recorded message or even automatically alert the police. Software agents could also solve the difficultly of monitoring all the CCTV cameras and provide a better assurance that the loudspeakers are used objectively and flawlessly.

However, once again, software agents potentially require separate legislation (Schermer, 2007) and the technology is likely not yet sophisticated enough. Moreover, the decisions of a software agent may classify as an "automated individual decision" and, therefore, should set off the safeguards of Council Framework Decision 2008/977/JHA.[447]

In a "symmetrical surveillance" scheme for CCTV systems (Goold, 2006), the data on the use and deployment of CCTV loudspeakers, including the messages used, where, when and by whom, would be easily and readily available to the public on the Internet. This could further deter the abuse of the intrusive power of CCTV loudspeakers by operators, address the concern over "who watches the watchers" (Cockfield, 2003), and reduce the problem of the "unobservable observer" (Goold, 2006) or, more precisely, in the case of CCTV loudspeakers, the 'unobservable speaker'.

The control room supervisor should also be responsible for monitoring the use of CCTV loudspeakers by the operators. If any operator uses the loudspeakers in an unwarranted manner, such as for 'cheap thrills' or in a racial discriminatory manner,[448] he or she may be subject to disciplinary action, including, but not limited to, dismissal. Based on the ***principle of enforcement***, an oversight/supervisory committee should be established to oversee the proportional and warranted deployment and use of the CCTV loudspeakers on a nationwide scale, ensuring individual liberty, public peace and the right to be left alone out in public is better preserved.

---

447 Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters (30.12.2008), article 7.

448 As Norris and Armstrong point out, evidence increasingly shows that CCTV operators are already using the surveillance capabilities of CCTV cameras in a racial discriminatory manner (1999, pp. 110-111).

6.10 CONCLUDING REMARKS

The deployment and use of CCTV microphones and loudspeakers, in conjunction with other technologies, could potentially enhance the ability of CCTV cameras to prevent and fight crime and serious anti-social behaviour. Therefore, CCTV microphones and loudspeakers ought not to be completely banned.

However, without an unambiguous understanding of the scope of privacy in public and/or the necessary regulations on the development, deployment and use of CCTV microphones and loudspeakers, there is no assurance that our legitimate rights and freedoms will not be unreasonably and disproportionally intruded upon. Until these regulations are in place and put into effect, there are alternative privacy-friendly devices and means of preventing and fighting crime and anti-social behaviour already in existence.

Indeed, being out in public entails a much lesser degree of privacy, and those who engage in unlawful, wicked or serious anti-social behaviour, whether thieves, murderers, vandals or terrorists, substantially lose their right to be left alone. However, the legitimate governmental interest in curtailing crime and anti-social behaviour should not mean that our conversations out in public may simply be recorded or citizens may be publicly humiliated into behaving 'correctly'.

7 HUMAN-IMPLANTABLE MICROCHIPS: Location-awareness & the dawn of the Internet of Persons

7.1 CHAPTER INTRODUCTION

In an age of sophisticated location-based services (LBS)[449] and GIS, and at the dawning of the 'ubiquitous information society' as a result of RFID, the development and deployment of HIMs, and their prospective added linkage to GPS satellites, for human identification and tracking purposes, may have certain security, health, convenience and commercial benefits. However, HIMs also raise serious concerns whether or not the existing legal framework in the US is adequately capable of protecting the core principles of privacy protection and democratic freedoms.

Section 7.2 explains the technology behind human-implantable microchips. Section 7.3 describes the social and privacy implications of the identification and tracking capabilities of human-implantable microchips and other location-based services. Moreover, the section focuses on how human-implantable microchips can change the nature of the public space and the way we view our bodies. However, for the most part, the ethical or moral issues surrounding the deployment of HIMs are not discussed. Section 7.4 outlines the security gains of human-implantable microchips. Section 7.5 outlines the security drawbacks and risks of human-implantable microchips. Section 7.6 reveals the scope of the actual deployment of human-implantable microchips in the US and abroad, and illustrates the potential further deployment. Section 7.7 describes the possible alternatives to human-implantable microchips. Section 7.8 gives an overview of the statutory law, case law, administrative decisions and soft regulations in the US of special relevance to human-implantable microchips. However, the medical, consumer and financial privacy issues associated with human-implantable microchips are

449 Location-based services and applications allow users to benefit from services that make use of their accurate physical location accessible via, for example, cell phones, smartphones or mobile computing devices (MCDs), and include services to locate in real-time another person or to locate a place or object, such as the whereabouts of the nearest automated teller machine (ATM). Other types of LBS include emergency services, real-time traffic information, route information, and tourist information.

not thoroughly dealt with here[450]. Instead, the focus is on the privacy issues associated with the *identification and tracking capabilities*[451] of human-implantable microchips (RFID/GPS implants) and the legality of processing location information. Section 7.9 assesses and highlights the relevant deficiencies and dilemmas of the US legal framework in terms of safeguarding privacy and civil liberties, with regards to the potential deployment and use of human-implantable microchips. Section 7.10 proposes relevant policy and legislative recommendations to enhance the US legal framework. Section 7.11 concludes with some ending remarks.

For the purposes of this dissertation, HIMs are implantable RFID tags (hereinafter known as "RFID implants") and/or implantable GPS receivers/transponders (hereinafter known as "GPS implants") marketed or sold for human-implantation.[452] *HIMs, for the specific purposes of this dissertation, however, will not include biosensors, sensory amplifiers, cortical implants, cochlear implants, or any other medical device, including Proteus Biomedical's implantable ChipSkin™ or "chip in the pill" technology or the "SmartPill", which adds intelligence to implanted medical devices or medication, nor does it include micro-electrode arrays, wireless implantable sensors or implantable nanomachines.*

7.2 RFID/GPS IMPLANTS AND THE TECHNOLOGY BEHIND THEM

7.2.1 RFID implants

More than four decades ago, Westin had already predicted that "[e]xisting microminiaturized transmitters the size of a pinhead might be coded with an identification number,

[450] The legislation and regulations that apply to credit and debit cards, such as the Truth in Lending Act and Regulation E, will likely apply, while consumer privacy will be protected to the extent that it is protected under existing laws, such as the Gramm-Leach-Bliley Act and the Fair Credit Reporting Act. see Willingham, Kristina M. Scanning Legislative Efforts: Current RFID Legislation Suffers from Misguided Fears, North Carolina Banking Institute, Volume 11 (2007), pp. 313-341.

[451] While to some extent medical privacy issues are touched upon, it is not the central issue that is addressed.

[452] HIMs could also be referred to as "ICT implants". see Weber, Karsten. The Next Step: *Privacy Invasions by Biometrics and ICT Implants* (Ubiquity, Vol. 7, Issue 45, 2005), available at: www.acm.org/ubiquity/views/pf/v7i45_weber.pdf; OPINION OF THE EUROPEAN GROUP ON ETHICS IN SCIENCE AND NEW TECHNOLOGIES TO THE EUROPEAN COMMISSION, Opinion No. 20, Adopted on 16/03/2005.

enclosed in a permanent capsule, and implanted under the skin by a simple and painless surgical operation" for locating individuals (1967, p. 86). At that time, this might have seemed somewhat science fiction, but today this is indeed taking place.

Animals and physical objects have been identified and tracked in supply chain processes using radio frequency identification (RFID) technology for some time now. However, we have moved beyond the use of RFID to expedite logistics and facilitate supply chain management. Now, RFID is becoming a technology of choice for identifying humans. For instance, in the EU, as Eurostat revealed, in 2009 'person identification' (albeit, not implanted) accounted for 56% of all RFID use by enterprises.[453]

RFID is a type of "automatic identification technology" (AIT) or "automatic identification and data capture" (AIDC) technology,[454] which provides the "means of [electronically] identifying things or individuals, collecting data about them, and automatically causing that data to be entered into a computer system, with no human interaction".[455] A RFID tag or microchip is the combination of an antenna coil and a silicon microchip with basic modulation circuitry and memory, and RFID tags can range from a fraction of a millimeter to several millimeters or centimeters.

In a way similar to CDs, RFID tags can be developed as read-only, read-write or write once, read many (WORM). Read-only tags contain data, which is added or 'written' during their manufacture, which cannot be changed, removed or augmented, similar to an original CD album commercially sold. Additional data can later be 'written' on read-write tags by command pulses from a read-write RFID interrogator/reader. The data on WORM tags is not set during their manufacture, but rather set the first time it is used, similar to a blank non-rewritable CD.

RFID tags can either be passive or active. The latter are powered by a battery and constantly transmit their data, while the former are activated by the radio frequency (RF) signal emanated from RFID readers/interrogators and only transmit their data when activated. In order to allow multiple RFID tags to be read simultaneously by a single reader without their signals interfering with each other, the reader employs an anti-collision algorithm, which controls access to the shared radio channel or frequency (Floerkemeier et al., 2005, p. 3).

[453] For further information, see Eurostat news release at: http://epp.eurostat.ec.europa.eu/cache/ITY_PUBLIC/4-19012010-BP/EN/4-19012010-BP-EN.PDF

[454] Other types of AIDC technology or AIT include: bar codes, QR Codes, optical character recognition, and biometric technology.

[455] The Use of RFID for Human Identify Verification, Report No. 2006-02, Data Privacy & Integrity Advisory Committee, Adopted 6 December 2006, p. 2, available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf

When a passive RFID tag is in the presence of an appropriate RF signal, emanated continuously by an RFID reader's antennae, it sends in response its stored data (ID number, etc.) to the reader using the reader's own carrier signal. The reader can range from inches to several feet away and the direct line of sight or physical contact between the tag and reader is not required. Passive RFID tags also do not need a battery since they are powered by the reader's signal.

Each time a RFID tag or RFID implant is read, a tag read event (TRE) is generated, which can automatically be registered and stored in a computer database. TREs can contain, in addition to the unique ID number, the antenna's ID number that read the RFID tag or RFID implant (i.e. the location of the RFID reader) and a timestamp.

A RFID implant is a silicon-glass encapsulated, passive and read-only RFID tag, which is normally injected into the right hand or upper right arm by a doctor or medical practitioner using a syringe. Neither surgery nor sutures are required. However, RFID tags can also be implanted into human molars.[456] To enable bonding to human tissue and thereby prevent migration, RFID implants are coated with a polymer. A signal, currently at a low frequency of 125 or 134 kilohertz (KHz), emitted by the antennae of either a fixed location or a wireless handheld RFID reader, remotely activates the RFID implant causing it to transmit its unique ID number (in the case of VeriChip's RFID implant a 16-digit number) back to the RFID reader, which in turn is either wirelessly relayed automatically to a computer or entered manually. The number then can be used to identify the individual and access his or her additional personal information via a computer database or on the Internet, such as medical or financial information or even biometric data, such as a digitized photograph or fingerprint. Typically, around 20 cm is the read range for the low frequency ban of 125-134 KHz, but it can go up to one meter.[457] Currently, the size of implantable RFID tags can range from 8 to 12 mm in length and 1 to 3 mm in diameter. RFID implants can hold anything from 56 to 512-plus bits of data. However, with the advancement of RFID technology, cloud computing and miniature microprocessors, RFID implants (HIMs) will only get smaller and gain augmented data, processing and communication capacities and will be increasingly linked to the 'cloud'.

---

[456] see Thevissen, Patrick., et al. *Implantation of an RFID-tag into human molars to reduce hard forensic identification labor* (F*orensic Science International*, Volume 159, 2006), pp. 33-39.

[457] OECD Policy Guidance on Radio Frequency Identification (2008), pp. 33-34.

VeriChip,[458] the only official distributor of human-implantable RFID microchips,[459] first marketed their product as a means of assisting doctors and nurses in emergency situations by providing patient information.[460] When an unconscious patient is administered into a hospital, the medical staff can employ an RFID reader. If the patient has a RFID implant embedded, the reader will indicate its unique 16-digit ID number, which can subsequently be entered manually or wirelessly transmitted to VeriChip's web-enabled database to access the patient's medical and personal information. If the hospital has indeed adopted the VeriMed Patient Identification System protocol in their emergency rooms, medical staff can immediately access the patient's identification and health record – information that can prove vital in an emergency situation.[461] VeriChip implantees can access, via the Internet, the Global VeriChip Subscriber service or VeriMed Registry or VeriMed Health Link System to add personal healthcare information to VeriChip's web-enabled database.[462] The VeriChip RFID implant is 11.1mm x 2.1mm and can hold up to 128 bits of information.

Moreover, VeriChip Corp. (currently known as PositiveID Corp.) has even taken the "capabilities of RFID implantable microchips beyond simple identification" to create the "GlucoChip", which "combines an embedded bio-sensor system on an implanted RFID microchip" (i.e. RFID implant) that enables glucose levels in the body to be measured in real-time.[463] Therefore, while PositiveID Corp. (formerly known as

---

[458] In 2009, VeriChip Corporation changed its name to PositiveID Corporation after completing its acquisition of Steel Vault Corporation. Throughout this dissertation, however, the company that created the first FDA approved RFID implant will still be known as VeriChip, in order to avoid confusion.

[459] But, VeriChip certainly did not invent the concept of HIMs. see, e.g., U.S. Patent. No. 4,706,689, Issued to Daniel Man on 17 November 1987, which describes a device designed to be implantable behind the ear of a human. The device transmits a signal intended to enable tracking of the implantee. The device operates continuously and is designed to be recharged through external contacts.

[460] As outlined later on, VeriChip has also marketed the use of its RFID implants for purposes beyond merely providing medical information when needed.

[461] In June of 2007, the American Medical Association concluded that implantable "[r]adio frequency identification (RFID) devices may help to identify patients, thereby improving the safety and efficiency of patient care, and may be used to enable secure access to patient clinical information". American Medical Association, CEJA Report 5-A-07, p. 4, available at: http://www.ama-assn.org/ama1/pub/upload/mm/467/ceja5a07.doc

[462] VeriChip and Microsoft have also entered into an agreement, whereby users of the VeriMed Health Link System will now be able to export their information to Microsoft's HealthVault. see Bacheldor, Beth. "Microsoft Partners With Implantable RFID Chip Maker VeriChip", *RFID Journal*, 2 December 2008, available at: http://www.rfidjournal.com/article/articleview/4477/1/1/

[463] see http://www.positiveidcorp.com/products_glucochip.html

VeriChip Corp.) has apparently stopped marketing the VeriChip implant, the company has changed the name to "GlucoChip" and integrated additional capabilities.

7.2.2 GPS implants

GPS tracking devices have also become an accepted tool of law enforcement agents to covertly track suspects or overtly track sex offenders and of business owners to track employees, while other location-aware devices, such as GPS-enabled mobile phones and their corresponding applications have also become extremely popular.

The GPS is a US space-based Global Navigation Satellite System (GNSS) that provides reliable positioning services to civilian users on a continuous worldwide basis. The GPS is made up of three parts: 24 satellites orbiting the Earth; monitoring stations on Earth; and the GPS receivers owned by end-users. GPS satellites transmit signals from space that are picked up and identified by GPS receivers. The GPS receiver in turn calculates or triangulates its own position every second or few seconds, consisting of current longitude, latitude, altitude and time, based on the readings from the satellites with an accuracy of a few feet or better anywhere on Earth.[464] GPS receivers alone do not disclose location information. However, when combined with data transmission technology or cellular phone technology, GPS receivers can disclose the geographic coordinates to another party.

GPS implants are the combination of the technology of GPS and cell phones, creating an enduring sub-dermal personal locating device (PLD). The GPS implant uses GPS to accurately locate itself and the cellular phone network to transmit its location. The cellular phone network enables the GPS implant to continue to function in areas such as underground subway tunnels. GPS especially has some problems in urban areas, indoors and other GPS-impaired environments that lack direct line-of-sight to GPS satellite signals. But, A-GPS (Assisted GPS) and, as proposed by Darren Murph, a so-called "GPS repeater" can enhance the ability of GPS devices to receive signals indoors, underground and in dense urban areas.[465]

The way in which GPS implants are meant to work is the following. GPS satellites send a signal to the implant which then in turn relays a radio signal via the cellular phone network, using a built-in transponder or General Packet Radio Service (GPRS)

---

[464] see the US Government website on GPS, available at: http://www.gps.gov

[465] see Murph, Darren. "Underground / indoor GPS repeater maintains your position" (Engadget, 21 February, 2007), available at: http://www.engadget.com/2007/02/21/underground-indoor-gps-repeater-maintains-your-position/

module, to “push” a stream of accurate real-time geographic coordinates to a monitoring station where it can be digitally stored on Internet servers or computer databases to form what Morris et al. (2004) have termed “digital trail libraries”.

GIS software can then plot the GPS implantee’s movements and convert or interpret geographic coordinates into understandable street addresses. Integrating hardware, software and data, GIS allows users to view geographic coordinates or data in different ways and reveal relationships, patterns and trends in the form of maps, reports and charts. There are three views: the database view; the map view; and the model view.[466]

Despite earlier reports that GPS satellites are deteriorating,[467] the system is instead currently undergoing a multi-billion dollar upgrade, which will gradually replace satellites, meant to significantly improve accuracy and deliver new capabilities in the future.[468] Besides, an alternative or complementary to GPS is ‘Galileo’, the European GNSS currently being established by the EU and European Space Agency (ESA), with scheduled completion by 2013. Similar to GPS, Galileo will be an open service to everyone. GPS and Galileo will be capable of operating together, allowing future interoperable multi-signal receivers to receive signals from both systems, which is also expected to improve accuracy and reliability.

For now, the GPS element, in particular, requires the implant to be considerably larger than ordinary RFID implants and requires considerable more energy. GPS implants could be powered by a thermo-couple circuit that produces voltage from the fluctuations in body temperature or electromechanically through the movement of muscles in the body.[469] Even more revolutionary, a small external power source, attached anywhere on the human body with electrodes and using the human body’s electrical conductive properties, could also possibly power the GPS implant.[470] Alternatively, however, as part of a Personal Area Network (PAN), RFID implants could perhaps

---

466 see the Guide to Geographic Information Systems, available at: http://www.gis.com

467 see Johnson, Bobbie. “GPS system ‘close to breakdown’” (The Guardian, 19 May 2009), available at: http://www.guardian.co.uk/technology/2009/may/19/gps-close-to-breakdown

468 see Hennigan, W.J. *GPS is getting an $8-billion upgrade* (Los Angeles Times, 23 May 2010), available at: http://articles.latimes.com/2010/may/23/business/la-fi-gps-20100523

469 see U.S. Patent No. 5,629,678, Issued 13 May 1997, describes an apparatus for tracking and recovering humans utilizing an implantable transceiver powered electromechanically through the movement of body muscle.

470 see U.S. Patent No. 6,754,472, entitled “Method and apparatus for transmitting power and data using the human body”, Issued to Microsoft Corporation on 22 June 2004. (Similarly, Xega, a security firm in Mexico, has also started offering HIMs that apparently send radio signals to a special GPS device carried by the implantee, which can then be used to determine the location of that person if he or she were to be kidnapped).

communicate with the GPS microchips and GPS applications already widely available within smartphones and, as a result, lower the energy requirements of HIMs.

7.3 LOCATION-AWARENESS AND THE DAWN OF *AN INTERNET OF PERSONS*

7.3.1 The capabilities of HIMs

The capabilities and privacy risks associated with HIMs are significant. Although VeriChip, for example, primarily markets their product (a RFID implant) for medical applications,[471] RFID implants can be used to identify and track/monitor the movements of living organisms, both human and animal.

However, as the staff of the Federal Trade Commission (FTC) rightfully point out, "RFID by itself is not a location-tracking technology".[472] There are significant infrastructure requirements. In order to enable RFID to track the movements of people, the widespread, strategic and registered placement of RFID readers, linked to computer databases, in synergy with RFID implants (or other RFID tags associated with persons one way or another), is required. Interoperable RFID readers, wirelessly linked to the Internet and positioned by public authorities and/or private entities at the entrance of airports, train stations, government buildings, stores/shopping centers, etc., throughout highways and cities, and attached to CCTV cameras, can enable the tracking of the daily movements of RFID implantees (or anyone for that matter in possession of a RFID tag coupled with personal information).

The potential widespread deployment of RFID-enabled mobile phones will only enhance that capability by increasing the number of RFID readers in the global infor-

---

471 However, VeriChip has promoted their RFID implant for other purposes.

472 RFID: Radio Frequency IDentification: Applications and Implications for Consumers: A Workshop Report From the Staff of the Federal Trade Commission [hereinafter called "FTC staff report on RFID"], FTC, March 2005, p. 3, available at: http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf
Moreover, RFID technology and its applications do not always present threats to privacy and personal data protection. Examples of non-threatening RFID applications may include document management, supply chain management and other Business-to-Business services.

mation system.[473] In addition, the RFID readers can be integrated with GPS technology, similar to the scheme developed by EarthSearch Communications. For the most part, the tracking capabilities of RFID implants are proportional to the number of readers deployed in public. On the other hand, Wi-Fi based RFID systems, like the technology pioneered by AeroScout,[474] and the use of a higher RF signal, can considerably reduce the number of RFID readers needed to track the movements of millions and millions of people (implantees).

Like GPS satellites, RFID technology and the corresponding infrastructure will also play a significant role in changing the nature of the public space. As Rob van Kranenburg explains, "the satellite infrastructure [GPS] creates connectivity from above. The RFID infrastructure creates connectivity from below".[475] While the GPS network, combined with the cellular network, can constantly relay an individual's exact location anywhere, RFID is more effective and convenient for tracking individual's movements within buildings. The Ubisense system, for example, using RF technology, can reveal the exact location in real-time of any number of individuals in huge complex sites within 15 cm of accuracy and render this information in 3D visualizations on screens.[476]

The capability of RFID technology to track movements indoors and reveal habits and relationships of individuals was already demonstrated ironically on the British TV show *Celebrity Big Brother*. RFID readers were installed by Wavetrend in numerous locations within the 'Big Brother house', while the housemates were made to wear RFID tags. Wavetrend's AssetTrace allow the show's producers to view on a screen the floor plan of the house and each participant's location in real-time. According to the show's producers, the scheme will enable the TV show's psychologists to interpret the

---

473 There is a real possibility that RFID readers will be integrated into most new cell phones within a couple years. see Lomas, Natasha. "RFID could be in all cell phones by 2010" (ZDNet News, 25 June 2009), available at: http://news.zdnet.com/2100-9595_22-315292.html; Nokia and Samsung have already unveiled RFID mobile phone readers, and there were rumors that the next-generation iPhone (v.4) will have a built-in RFID reader. These rumors are substantiated by the fact that Apple has applied for a patent for a touch screen RFID tag reader. However, as of June 2010, this has yet to manifest and the just released iPhone v.4 does not have a RFID reader. The reasons for the delay could be the uncertainties of manufacturers due to the privacy concerns, lack of adequate standards and legal deficiencies.

474 see AeroScout, available at: http://www.aeroscout.com/content.asp?page=SystemOverview

475 van Kranenburg, Rob. The Internet of Things: *A critique of ambient technology and the all-seeing network of RFID*, Network Notebooks 02, Institute of Network Cultures (2008), p. 18, available at: http://www.networkcultures.org/_uploads/notebook2_theinternetofthings.pdf

476 see Ubisense, available at: http://www.ubisense.net/content/8.html

celebrities' behavior and question the housemates who have been voted off about their movements within the house.[477]

Essentially, RFID implants can broadcast the implantee's unique ID number, which may serve as a means of identification, to anyone or anything with a RFID reader within inches to several feet/meters away. The greater the radio frequency in which RFID implants operate, the greater the distance from which they can be read by RFID readers. The greater the 'read range' of RFID implants, the greater their capability to keep track of movements, and thus essentially the privacy-intrusive capability of RFID implants is, in part, directly proportional to the radio frequency.[478] However, a frequency higher than 125 or 134 KHz may be required to significantly improve the tracking capabilities of RFID implants, but not too high, as this would hamper the RF signal's capability of penetrating an implantee's flesh, since "low frequency signals penetrate liquids more easily"[479] and humans are mostly made up of water. Nevertheless, RFID readers with more powerful antenna could potentially read the RFID implants beyond their standard or nominal read range, known as the "rogue scanning range",[480] and the use of a second reader could "eavesdrop" on the RFID implant at a greater distance than the rogue scanning range.[481]

In addition to the distance at which RFID tags can be read, as the OECD Policy Guidance on Radio Frequency Identification also points out, the potential privacy invasion through the use of RFID is also likely to be proportional to the possibility of revealing "sensitive information about individuals through inferences and profiling", the degree of interoperability and the tracking capabilities.[482] With the increasing advancement of RFID technology, including augmented data, processing and communication capacities, the privacy-intrusive capabilities of RFID implants will equally increase.

---

477 see Swedberg, Claire. "RFID Works for Big Brother" (RFID Journal, 7 January 2009), available at: http://www.rfidjournal.com/article/articleview/4534/1/1; Savvas, Antony. "Celebrity Big Brother uses RFID technology to track housemates" (Computer Weekly, 6 January 2009), available at: http://www.computerweekly.com/Articles/2009/01/06/234068/celebrity-big-brother-uses-rfid-technology-to-track.htm

478 see OECD Policy Guidance on Radio Frequency Identification (2008).

479 *Ibid.*, p. 31.

480 see "A Holistic Privacy Framework for RFID Applications", Future of Identity in the Information Society, Simone Fischer-Hübner and Hans Hedbom (eds.)., Deliverable D12.3, p. 69, available at: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp12-del12.3.A_Holistic_Privacy_Framework_for_RFID_Applications_v2.pdf

481 *Ibid*.

482 OECD Policy Guidance on Radio Frequency Identification (2008), p. 53.

HIMs can also be integrated with other technologies. For instance, RFID implants and RFID readers can enhance the capabilities of CCTV surveillance systems. RFID readers attached to or located nearby CCTV cameras could potentially combine visual surveillance with database-linked surveillance capabilities, thereby enabling CCTV camera operators to identify and follow the individual they wish to observe. However, while this may be more practical than using face recognition software, extensive co-ordination between the relevant data controllers is required. RFID implants could also be potentially interfaced with Wi-Fi technology. VeriChip already began the process of interfacing their RFID implants with Wi-Fi, in order "to achieve an even higher level of system integration that collects location-based information".[483]

Generally, tags read events (TREs) can be anonymous at first, but can later be converted into personally identifiable location information. For example, the unique ID number of RFID implants can automatically be coupled with a debit or credit card when an implantee makes a purchase in a shop that contains RFID readers. Such information could later be used to identify and track the implantee and target personalized, real-time, location-based advertisements, either via nearby screens or via mobile phones, as the person passes by any RFID reader associated with the same shop or company.

Linking HIMs to the implantee's bank account, debit card or credit card number could also enable the use of HIMs to make cashless transactions,[484] which is perhaps why some correlate HIMs with the 'Mark of the Beast' as prophesized in the Bible.[485] When an implantee's right arm or hand is scanned, followed by the entering of a PIN, the transaction can be executed.[486] HIMs can, therefore, also enhance the ability of retailers and marketers to meticulously record the consumer habits of individuals.

---

483 see VeriChip Corp.'s 10-K Annual Report for the fiscal year ended 31 December 2007, p. 16, available at: http://www.sec.gov/Archives/edgar/data/1347022/000136231008001657/c72788e10vk.htm

484 ADS revealed at the ID World 2003 International Congress in Paris, France, the company's subdermal RFID solution called VeriPay, which allows the implant to be used to make payments. see McCullagh, Declan."Chip implant gets cash under your skin" (CNET News, 25 November 2003), available at: http://news.cnet.com/2100-1041-5111637.html

485 "He causes all, both small and great, rich and poor, free and slave, to receive a mark on their right hand or on their foreheads, and that no one may buy or sell except one who has the mark or the name of the beast, or the number of his name". (Revelation 13:16).

486 VISA and MasterCard have already developed and deployed contactless smartcards, which make use of RFID, such as MasterCard's PayPass card. Other examples include Exxon Mobil's SpeedPass. In an article, published by TIME Magazine in 1998, entitled "The Big Bank Theory" Joshua Cooper Ramo, et al., proclaimed, "Your daughter can store the money any way she wants--on her laptop, on a debit card, even (in the not too distant future) on a chip implanted under her skin". The question is will this prove true within the next ten years?

However, the concern over remotely tracking people's movements does not only pertain to RFID and/or GPS implants. Although HIMs are the ultimate person-locating device or generator/transmitter of location information, GPS enabled hand-held devices or smartphones and even traditional mobile phones are already capable of being used to track or locate users.[487] The risk is so high that the Secret Service strongly advocated that US President Barack Obama give up his Blackberry for security purposes, since there was a high risk that his location could be determined. Even the Bluetooth signal emitted from mobile phones can be used to track users, as demonstrated by Bath University's Cityware project.[488]

Moreover, RFID tags can be embedded in practically anything people buy or wear, from clothes, watches and shoes to items in a woman's purse such as lipstick, and, similar to RFID implants, can be used to track and identify persons (Albrecht and McIntyre, 2005). People throughout the day normally carry these items. RFID tags are already being embedded in a number of consumer goods. Equally, personally identifiable information (or personal data) can be linked to the unique numbers of the RFID tags embedded in these items when they are purchased using a credit or debit card.[489] As Linda D. Koontz, Director of Information Management Issues at the US Government Accountability Office (GAO), testified, "once a tagged item is associated with a particular individual, personally identifiable information can be obtained and then aggregated to develop a profile of the individual".[490]

7.3.2 Location information

HIMs can generate practically limitless amounts of location information on individuals. Here, location information, however, is not limited to where an individual lives or

487 The location of traditional cell phones can also be determined or "triangulated", albeit less accurately.

488 The discontinued Cityware project tracked mobile phone users at various locations to study patterns of how people move around cities. The participating users required a Facebook account and the Cityware application and needed to register the Bluetooth ID of their mobile phone. The researchers had set up nodes around the UK and in the US, which constantly scanned for Bluetooth-enabled devices in a given area, and then relayed information to servers, which compared the IDs of the devices with the enabled Facebook profiles. see "Bluetooth helps Facebook friends", (BBC News, 16 August 2007), available at: http://news.bbc.co.uk/2/hi/6949473.stm

489 see FTC staff report on RFID, p. 14.

490 Testimony Before the Subcommittee on Commercial and Administrative Law, Committee on the Judiciary, House of Representatives, PRIVACY: Key Challenges Facing Federal Agencies, Statement of Linda D. Koontz, Director of Information Management Issues, 17 May 2006, GAO-06-777T, p. 16, available at: http://www.gao.gov/new.items/d06777t.pdf

works and the street addresses thereof, but rather pertains to either information on their daily movements tracked and stored over a prolonged period of time ('mobility data') and/or their accurate, real-time, physical location at any given moment. For the purposes of this dissertation, location information includes, in addition to ordinary street addresses, both geographic coordinates and TREs.

Location information should be considered a category of personal information when it is personally identifiable or can later potentially be construed as such. Location information/data, as the EU's 'ePrivacy Directive' distinguishes in Article 2, is not identical to traffic data processed for the purpose of carrying out a transmission on an electronic communications network or for the billing thereof, but rather is data which indicates the geographic position of the terminal equipment of a user of a publicly available electronic communications service in order to provide a 'value added service' (or location-based service).[491]

The intrinsic market value of the location information generated by HIMs in the so-called 'information age' could potentially result in HIM service providers and/or data controllers succumbing to lucrative temptations and disclosing their customer's location information to a variety of third parties, such as insurance companies, retailers, marketers, data brokers and even law enforcement agencies. As Masters and Michael argue, "[t]he main temptation will be in the value of the data and how it can be used not only to sell value-added services but separate service-sets that rely on location information" (2006, p. 32). Under a 'surveillance-for-profit' scheme, locations, for example, where one travels, eats and shops on a daily basis are just a few examples of information that is very valuable to retailers and marketers (Karim, 2004, p. 495). Location information can, for example, enable location-based advertising (LBA) in real-time. Thus, location information has a huge potential of becoming a key asset within the 'knowledge-based economy' of tomorrow's 'ubiquitous information society'. The location information generated by smartphones has already begun to be provided to marketers to target advertisements based on a person's real-time location and travel patterns,[492] and TechnoCom Corporation, for example, has launched SpotOn GPS, a LBA platform for mobile phones.

However, personally-identifiable location information, as a whole, is considerably more privacy-intrusive than simply revealing the places where a person, on a daily ba-

---

491 The ePrivacy Directive explicitly regulates 'location data', requiring that the use of non-anonymous location data is particularly restricted to the extent necessary to provide the value added service, and clarifies the scope of the required informed consent (Article 9), and the scope of use without informed consent.

492 see Clifford, Stephanie. "Advertisers Get a Trove of Clues in Smartphones" (The New York Times, 11 March 2009), available at: http://www.nytimes.com/2009/03/11/business/media/11target.html

sis, shops or eats. As emphasized by the EU's Article 29 Working Party, the processing of location information is a particularly sensitive matter.[493]

7.3.3 Social and privacy implications

Indeed, location information can reveal not just where an individual travels, but potentially more sensitive information associated with where he/she has been, including a person's consumer habits and more private or personal affairs and activities. For example, as Jack Dempsey, currently Vice President for Public Policy at the Center for Democracy and Technology, inquires,

> What if your insurer finds out you're into rock climbing or late-night carousing in the red-light district? What if your employer knows you're being treated for a sexually transmitted disease at a local clinic? The potential is there for inferences to be drawn about you based on knowledge of your whereabouts.[494]

An experiment, carried out by Michael et al. (2006), demonstrated the sensitivity of location information. This study involved a participant who had their daily movements tracked for just two weeks. Each day during the two-week study, the participant carried a Magellan Meridian Gold handheld device either in a bag he carried around or in his pocket. The GPS device was setup to collect location data every three seconds. At the end of each day this data was uploaded into the GIS software "DiscoverAus Streets & Tracks". The study showed that tracking a person's movements over a period of time is relatively easy and can create a detailed profile of that person, including where he/she lives, works and engages in social activities, simply based on his/her daily travel routines (see Michael et al., 2006). As partly demonstrated in a more recent study, involving mobile phone users,[495] a person's movements tracked over a specific period of time

493 Article 29 Working Party, Opinion on the use of location data with a view to providing value-added services, November 2005 (WP 115), available at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp115_en.pdf

494 Romero, Simon. "Location Devices' Use Rises, Prompting Privacy Concerns" (New York Times, 4 March 2001), available at: http://query.nytimes.com/gst/fullpage.html?res=9E04E1DC123BF937A35750C0A9679C8B63&sec=&spon=&pagewanted=print

495 The whereabouts of more than 100,000 mobile phone users were tracked in an attempt to build a comprehensive picture of human movements. see Fildes, Jonathan. "Mobile phones expose human habits" (BBC News, 4 June 2008), available at: http://news.bbc.co.uk/2/hi/science/nature/7433128.stm

can be used to construct a profile of that person. These profiles, for example, can be used by the private sector for conducting market research and categorizing people and can also be useful for law enforcement agencies. Nevertheless, the privacy implications of tracking a person's movements and/or disclosing a person's location information also depend, to a certain point, on the type of activities that person engages in.

The ability of HIMs (or simply RFID tags) to identify/track individuals can thus lead to the development of profiles based on their movements and whereabouts. These studies have also shown that location information can be used for analyzing an individual's past movements in order to potentially determine a person's future movements. Even an individual's social interactions/social relationships can be potentially determined.[496] Location information, as a result, significantly further adds to the capability of creating "digital dossiers" on every person (Solove, 2004) in possession of a mobile phone/smartphone or implanted with a HIM.

Furthermore, since implantees will essentially not know when their RFID implant has been read and by whom, they must then bear an even greater risk of losing control of their personal data, if the relevant safeguards are not implemented to prevent this from happening.

The widespread deployment and use of RFID implants (or RFID tags) and RFID readers, whereby the implants/tags become a critical element in the granting or denying of physical access or the granting or denying of certain advantages, could also potentially add to the "digital divide"[497] and broaden discrimination in the digital age, as the non-implanted are faced with increasing disadvantages in a ubiquitous information society. However, since the digital divide is mostly an issue, at present, of not being able to afford the technology, in addition to not knowing how to use it, and RFID technology in general is rapidly becoming cheaper and is very easy to use, RFID implants will not necessarily add to the digital divide. But, if the people who refuse to be implanted are increasingly disadvantaged and discriminated against, and the law does nothing about it, then RFID implants will indeed rapidly add to the digital divide.

---

[496] *Ibid.*

[497] There is little consensus over the overall definition of the term "digital divide", but it essentially refers to the growing gap between those who have access to ICT and those who do not or the difference between the "haves" and the "have-nots" of ICT (see Hilbert, 2011, p. 5). Hilbert (2011) argues that the "[d]ifferences in definitions arise because scholars distinguish between (1) the kinds of Information and Communication Technology (ICT) in question; (2) the choice of subject; (3) diverse attributes of the chosen subjects; and (4) levels of adoption, going from plain access to effective usage with real impact" (p. 2). see Hilbert, Martin. *The end justifies the definition: the manifold outlooks on the digital divide and their practical usefulness for policy-making* (Telecommunications Policy, Volume 35, Issue 8, 2011), pp. 715-736, available at: http://martinhilbert.net/ManifoldDigitalDivide_Hilbert_AAM.pdf

While there are already valid concerns over the privacy threats of RFID, there are lots of unknowns. The need for further validating these threats can only come from the deployment of RFID applications. However, applying the *precautionary principle* here would imply that any potential widespread deployment of RFID implants should be put on hold, even before there is hard evidence concerning their tracking capabilities, until we are certain of all the privacy and social implications and the means and preconditions for addressing or preventing them.

7.3.4 A means of control

Human identification and tracking goes beyond privacy, serving as a powerful means of control. As Mark Weiser asserts, in referring to ubiquitous computing, "the problem, while often couched in terms of privacy, is really one of control".[498] If left unchecked, HIMs could pose a serious threat not just to privacy, but also to liberty and human dignity, as the European Group on Ethics in Science and New Technologies (EGE) equally points out.[499] As Melvin Gutterman further asserts:

> [t]he ability to move about freely without constant supervision by the government is an important source of individual liberty that must be addressed. A fear of systematic observation, even in public places, destroys this sense of freedom (1988, p. 706).

HIMs, or RFID technology in general, could have a 'chilling effect' on the freedom of movement, whereby people, concerned that their movements could be tracked and recorded, self-impose limitations on where they actually travel. Even worse, RFID implants could lead to controlled or restricted movement. For example, if RFID implants are used as travel passes for mass public transportation, a person could easily be electronically and remotely denied access. Contactless smart cards are already widely used and could similarly be used to restrict access to mass public transportation. RFID implants (or RFID embedded ID cards/passports) could also have a 'chilling effect' on the freedom of association, since government agents could potentially use RFID

498 Weiser, Mark. T*he Computer for the Twentieth-First Century* (Scientific American, Vol. 265, No. 3, September 1991), pp. 94-104.

499 OPINION OF THE EUROPEAN GROUP ON ETHICS IN SCIENCE AND NEW TECHNOLOGIES TO THE EUROPEAN COMMISSION, Opinion No. 20, Adopted on 16/03/2005.

readers to deliberately determine who is present at a demonstration. Unfortunately, however, these potential threats to personal freedom, posed by RFID and GPS, are being ignored, for the most part, by human rights and civil rights organizations and within human rights reports.

HIMs could serve as a powerful tool of mass control and mass management. For Dobson and Fisher (2003), electronically tracking people's movements and generating location information can lead to a "new form of slavery characterized by location control" or what they term "geoslavery".[500] Herbert (2006) similarly links human tracking to "geoslavery" and further associates the mandatory implantation of identification and tracking devices to slavery control mechanisms, such as branding.[501] Whether or not HIMs (or any other personal location-tracking device) will lead to "geoslavery", their widespread deployment could certainly bring about mass categorization.

In essence, if left unchecked, HIMs could be the last drop in the bucket needed to give rise to an age where omnipresent scrutiny and continuous, real-time surveillance is commonplace and limitless, a society where there will in effect be truly *nowhere to hide* in a global, automated, digital information surveillance-tracking grid that will become increasingly impossible to escape.[502]

7.3.5 Internet of Persons

Proponents of RFID and major investors behind its development and deployment envision the integration or 'bridging', so to speak, of the physical and virtual/digital world in what is now commonly known as the "Internet of Things" (IoT).[503] The IoT is defined as a "network of interconnected objects, from books to cars, from electrical appliances to food".[504] In a full-blown deployment of IoT, billions of physical objects are embed-

---

500 see Dobson, Jerome E. and Fisher, Peter F. *Geoslavery* (IEEE Technology and Society Magazine, 2003).

501 In linking mandatory RFID/GPS implants to a form of slavery, Herbert (2006) also argues that the Thirteenth Amendment of the US Constitution could serve as a basis of prohibiting any mandatory implantation.

502 see e.g. O'Harrow, Robert. *No place to hide* (Free Press, 2005).

503 see the First International Conference on the Internet of Things, Adjunct Proceedings, available at: http://www.iot2008.org/adjunctproceedings.pdf

504 COM(2009) 278 final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Internet of Things – An action plan for Europe, p. 2.

ded with RFID tags and assigned, for instance, Electronic Product Codes (EPCs),[505] allowing these objects to be identified and tracked in real-time either in a closed or open network.[506] When an RFID reader reads or interrogates an RFID tag embedded in an object, the EPC number is communicated to computers or mobile devices running relevant middleware, which can then use EPCglobal's Object Name Service (ONS), an automated networking service based on the Domain Name Service (DNS), which directs objects (instead of computers) to websites/web-based databases, in order to identify and track the object and enable access to the stored information on the object.[507] This information can include, in addition to other general product information, its location history or TREs based on the last occasions where the object's embedded RFID tag was read. Specific locations, such as a warehouse, shop or even a store shelf, can also be electronically identified using a Global Location Number (GLN), giving rise to the so-called "Internet of Places".[508] As pointed out in the OECD paper on "RFID: Drivers, Challenges and Public Policy Considerations", "the information infrastructures associated with RFID, in particular with UHF [ultra high frequency] RFID, will increasingly be accessed across IP networks, private intranets and the public Internet".[509]

Essentially, the data from RFID tags can be captured by RFID readers and wirelessly transmitted to computer databases over a network, stored on a server and made accessible anywhere in the world via the Internet, using a web-based application or even a search engine. The objects could then potentially be converted into what Bruce Sterling refers to as "spimes", objects that are location-aware, self-registering and uniquely

[505] EPCs, first developed by MIT's AutoID Center, are basically standardized codes for RFID tags. If RFID tags indeed eventually replace bar codes completely, as RFID technology advances and becomes cheaper to reproduce, then, as generally purported, EPCs could one day replace Universal Product Codes (UPCs). see Grossman, Lisa. "New RFID Tag Could Mean the End of Bar Codes" (Wired, 26 March 2010), available at: http://www.wired.com/wiredscience/2010/03/rfid/

[506] The assigning of IP addresses to objects has called into question the feasibility or rationale of considering IP addresses as personal data.

[507] For further explanation, see "Object Name Service (ONS), Version 1.0", EPCglobal Ratified Specification, October 4, 2005, available at: http://www.gs1.org/gsmp/kc/epcglobal/ons/ons_1_0-standard-20051004.pdf

[508] An "Internet of Places" is "where information specific to places can be readily picked up by devices and users in specific locations". see Cooper, Joshua and Anne James. *Challenges for Database Management in the Internet of Things* (IETE Technical Review, Vol. 26, Issue No. 5, August 2009), available at: http://tr.ietejournals.org/text.asp?2009/26/5/320/55275

[509] OECD (2006), "Radio-Frequency Identification (RFID): Drivers, Challenges and Public Policy Considerations", OECD Digital Economy Papers, No. 110, OECD Publishing, p. 18.

identifiable, and thus traceable in space and time.[510] With the gradual transition from IPv4 at 32 bits to IPv6 at 128 bits, there will be more than enough IP addresses for practically every single object and human on Earth.[511] On the whole, such a scheme could bring about 'ubiquitous positioning' or an "everyware" world.[512]

IoT is considered an integral part of the so-called "Future Internet" and is widely supported by industry stakeholders and other actors. IoT is also receiving public funding and widespread deployment is expected within the next several years. The IP for Smart Objects Alliance (IPSO Alliance), whose members include Cisco, Google and Intel, is a testament to the backing of the ICT industry's major players towards IoT and using IP as the network for the connection of personal and household 'smart' objects/devices.[513] Interesting enough, CIA Director David Petraeus discussed about the emergence of the IoT and the transformational ability of these smart devices to help the CIA execute their clandestine activities and gather immense quantities of geolocation data on individuals. Petraeus explained that "items of interest will be located, identified, monitored, and remotely controlled through technologies such as radio-frequency identification, sensor networks, tiny embedded servers, and energy harvesters – all connected to the next-generation internet using abundant, low-cost, and high-power computing".[514]

While the deployment of RFID is spreading and the industry is growing, IoT is still, nonetheless, a promising vision and currently not a reality.[515] It will also require a vast amount of additional data storage space, which is already an issue.[516] In spite of this, IoT

---

510 Sterling, Bruce. *Shaping Things* (MIT Press, 2005).

511 For further explanation see *Embedded, Everywhere: A Research Agenda for Network Systems of Embedded Computers*, Report from the Committee on Networked Systems of Embedded Computers, Computer Science and Telecommunications Board, National Research Council (National Academic Press, Washington, DC, 2001).

512 see Greenfield, Adam. *Everyware: The Dawning Age of Ubiquitous Computing* (New Riders Publishing, 2006).

513 "Smart objects" are essentially objects that are location-aware, possess processing capabilities and are able to 'communicate' with other objects.

514 Ackerman, Spencer. "CIA Chief: We'll Spy on You Through Your Dishwasher" (Wired blogs, Danger Room, 15 March 2012), available at: http://www.wired.com/dangerroom/page/2/

515 For instance, according to a survey in 2009 conducted by Eurostat, only 3% of enterprises in the EU27 use RFID technology. see Eurostat news release at: http://epp.eurostat.ec.europa.eu/cache/ITY_PUBLIC/4-19012010-BP/EN/4-19012010-BP-EN.PDF

516 see a special report on managing information from the Economist, titled "Data, data everywhere", Feb. 2010.

has already called into question the adequacy of the current legal framework in the US and the EU and the potential need for new legislation and/or a new governance model.[517]

But, we are now witnessing just the beginning of this location-aware revolution. As the ultimate vehicles of LBS and location awareness, HIMs could take us to the next level – an 'Internet of Persons'. In the same way RFID tags will usher in IoT, RFID implants will carry on the evolution of the Internet, and could ultimately bring about an "Internet of Persons" (see Figure 1), giving a whole new meaning to being inter-connected to one another or to 'networked individuals' or 'social networking' in tomorrow's ubiquitous information society. This evolution is arguably only a natural development with the growing trend of increasing mobility, ubiquity, traceability, identifiability and heterogeneity of components of the information society, and the growing enterprise for achieving unlimited storage space, bandwidth and Internet access points.

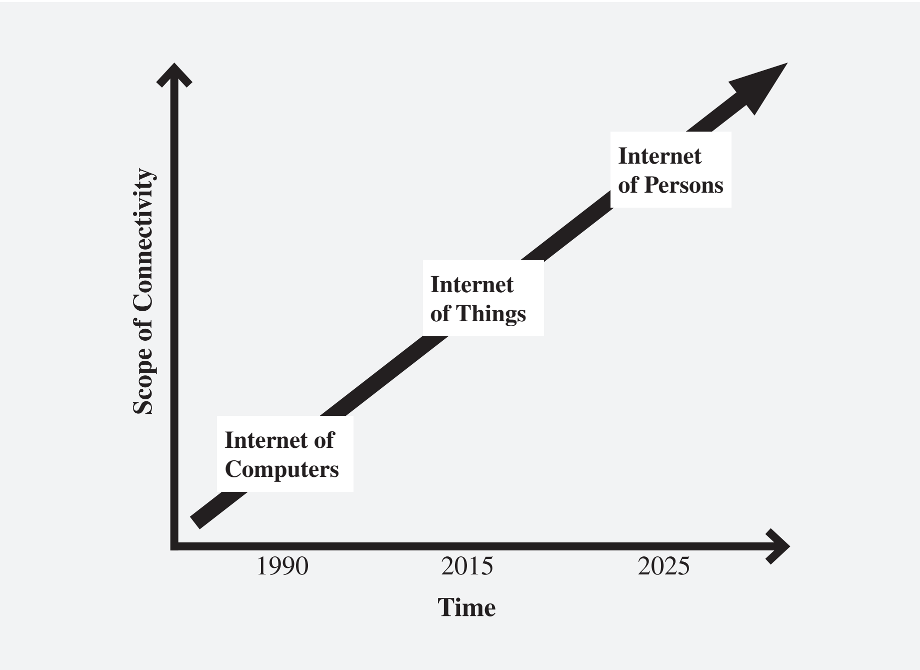

Figure 1: Potential evolution of the Internet

[517] see, for further discussion, for example: Weber, Rolf H. I*nternet of things – Need for a new legal environment?* (Computer Law & Security Review, Volume 25, Issue 6, November 2009), pp. 522-527.

RFID implants, assigned IP addresses and interfaced with the Internet, could in actuality link implantees with the virtual space, breaking the boundaries between the biological and the digital, and indirectly between each other.[518] The "Internet of Persons", for instance, could be based on the EarthSearch Communications' AutoSearchRFID unique solution, which combines data from RFID readers with GPS transmitters' real-time, location-reporting capabilities. While the system was developed for tracking goods or assets, a similar system could be used for RFID implantees. In any case, the TREs, together with the location information of the RFID readers, could be communicated to servers and made available via the Internet (see Figure 2).

As RFID or GPS implantees are transformed into two-way transmitters of information, both emitting as well as receiving data, and active generators of information, rather than passive receivers, "there is no more *we* as in we human beings, the "we" is an information space like any other" (van Kranenburg, 2008, p. 18). Implantees will become one with the global information space and part of the Internet, changing the nature of the human body. This would potentially mark the beginnings of "Internet-enabled people", a concept Vinton Cerf[519] envisaged more than a decade ago,[520] which could enhance the "web presence" of people, meaning that people will become accessible via the Internet through the automatic correlation between a web resource and their physical location, as envisaged by the Hewlett Packard's Internet and Mobile Systems Laboratory.[521] Already, an individual in the US has become the first person to be implanted with a pacemaker connected wirelessly to the Internet that can transmit

518 Already, in Japan, cattle have their own IPv6 addresses, enabling farmers to identify and track the cattle throughout the entire production lifecycle.

519 Vinton Cerf, often called "the father of the Internet", was instrumental in the creation of email, the development of TC/IP technology and the founding of the Internet Corporation for Assigned Names and Numbers (ICANN), which he chaired for seven years. At present, Cerf is Google's Chief Internet Evangelist.

520 Cerf, Vinton. "What Will Replace The Internet?" (TIME Magazine, 19 June, 2000), available at: http://www.time.com/time/magazine/article/0,9171,997263,00.html
(In the same article, Cerf gives the following example of the conception of Internet-enabled people. "The speech processor used today in cochlear implants for the hearing impaired could easily be connected to the Internet; listening to Internet radio could soon be a direct computer-to-brain experience!").

521 see Kindberg, Tim., et al. *People, Places, Things: Web Presence for the Real World* (Internet and Mobile Systems Laboratory, HP Laboratories Palo Alto, HPL-2000-16, February, 2000), available at: http://www.hpl.hp.com/techreports/2001/HPL-2001-279.pdf

information to her doctor.[522] RFID implants and the corresponding infrastructure could change not just our relationship and interaction with objects, electronic devices, public or private infrastructure and with each other, but also how we view ourselves and our bodies, now merged in a networked 'intelligent' environment. RFID implants, as technologies of human enhancement,[523] could thus eventually play a significant early role in the transhumanism movement.[524]

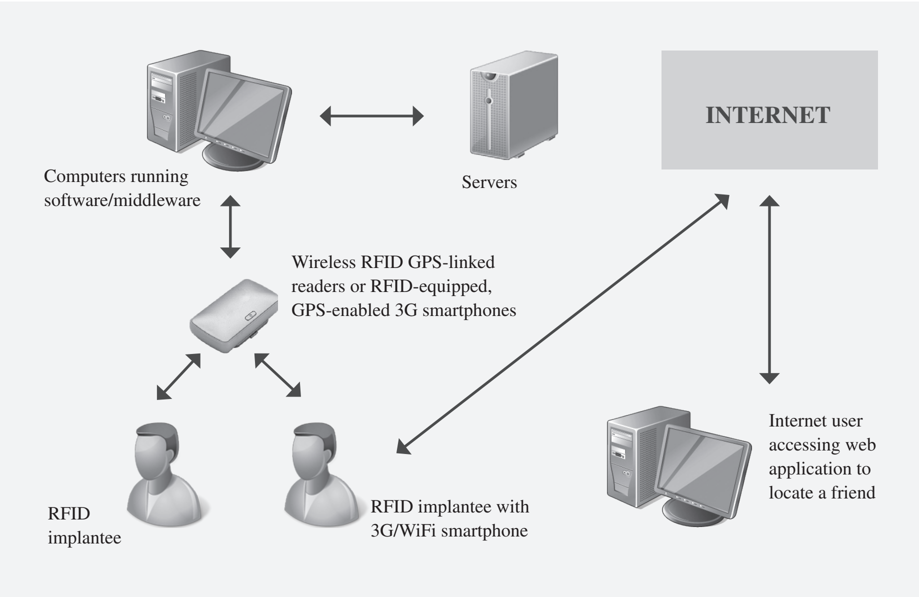

Figure 2: Internet of Persons

---

[522] Gruber, Ben. "First Wi-Fi Pacemaker in the US gives patient freedom" (Reuters, 10 August 2009), available at: http://www.reuters.com/article/idUSTRE5790AK20090810
Such a move is yet another example of the trend of increasing convergence of ICT and life sciences. see Weber, Karsten. *The Next Step: Privacy Invasions by Biometrics and ICT Implants* (Ubiquity, Vol. 7, Issue 45, 2005), available at: www.acm.org/ubiquity/views/pf/v7i45_weber.pdf

[523] The human enhancement abilities include, for example, the ability of implantees to automatically open doors and to pay for items.

[524] Transhumanism refers to the potential future merger of man and machine, what Ray Kurzwell and others refer to as "singularity", which also describes the era when artificial intelligence is equal to that of human intelligence. Transhumanism aims to augment human capabilities. HIMs are merely just the beginning.

Since HIMs can be interfaced with the Internet, there is the possibility of implantees being able to choose via a web application to automatically have their real-time location information posted on their social networking webpage or blog or even perhaps sent via services such as Twitter,[525] which would mean that a person's location information could be publicly available to anyone with access to the Internet. This information could thus also potentially be searchable on a search engine, such as Google. This would lead to what the Royal Academy of Engineering terms "Google spacetime",[526] whereby the location of a specified individual at some particular time and date can be searched on Google or another search engine, essentially again converting people into Sterling's "spimes" (2005). Even more, similar to Alcatel-Lucent's touchatag solutions (formerly known as Tikitag) and the concept of 'augmented reality', when a RFID implant is read by an RFID-enabled smartphone, for instance, the relevant implantee's personal website or social networking webpage could be launched on a smartphone, tablet PC or other MCD.[527]

While RFID implants can move us beyond today's Internet and past IoT, GPS implants can propel us beyond today's location-aware applications. GPS implants can improve the ability of being automatically notified of the location of a friend if and when he or she is within a certain distance nearby or being able to look up a friend's real-time location, regardless if RFID readers are present, via the Internet using, for instance, a smartphone.

7.3.6 Nearly there

The path towards the ultimate location-aware world that HIMs promise has already been initiated. A continuous wave of GPS-equipped smartphones and tablet PCs and a multitude of GPS tracking devices or personal locating devices (PLDs)[528] and servic-

525 Foursquare, a location-based social application, already enables users to automatically integrate their location "check-ins" with their tweets on Twitter.

526 *Dilemmas of Privacy and Surveillance: Challenges of Technological Change* (The Royal Academy of Engineering, London, 2007), available at: http://www.raeng.org.uk/policy/reports/pdf/dilemmas_of_privacy_and_surveillance_report.pdf

527 Already, the Astonishing Tribe, a Swedish mobile software developer, has developed software, which runs on camera-equipped smartphones, that can recognize a person's face and then launch links to that person's social networking websites on a smartphone/mobile device. The system integrates facial recognition, augmented reality and social networking. This development has been dubbed "augmented ID". For more info, see http://www.tat.se

528 see section 7.7 for an outline of the multitude of GPS tracking devices and PLDs (and corresponding services), which have recently hit the market and may serve as an alternative to GPS implants.

es[529] have hit the market over the past couple years, and the LBS market is also growing at a remarkable rate. In addition, the location-aware and processing capabilities of the microchips for smartphones are continuously advancing.[530]

As a result, millions of people are walking around with a device (i.e. a smartphone), albeit not implanted, but rather carried around in their pocket or purse, that can accurately pinpoint, track and transmit where they are at all times and, with a location-aware application, use that location information, in combination with web-based data, to find out what and who is nearby or provide other LBS.[531] The iPhone and Google's Android smartphones have a multitude of applications that tap into the available location information generated via GPS or the available cell phone data.[532] Even applications, such as games, that do not require location information to serve their purpose collect location information. Likewise, the Palm Pre smartphone, for example, transmits the user's location information back to Palm's servers without the user's permission and even when no location-aware application has been activated on the Pre, as programmer Joey Hess discovered.[533] The same was also later discovered about Google's Android smartphones and Apple's iPhone.[534]

Google has already launched an "Add Location" feature, which automatically adds location information to the sender's signature in Gmail, but this is based on the sender's device IP address as opposed to geographic coordinates derived from GPS. Develop-

---

529 Personal locating services include, for example, OnStar's "Family Link" service, which allows for vehicles equipped with OnStar to be tracked and authorized individuals to monitor the vehicle movements via the OnStar's website.

530 For instance, Broadcom has began to market the 4752 microchip for smartphones that can pinpoint the phone's location with ultimate precision, potentially within a few centimeters both outdoors and indoors, by receiving GPS, cell-phone and Wi-Fi signals and also input from gyroscopes, altimeters, etc. For further information, see Mims, Christopher. "A new microchip knows just where you are, indoors and out"
(MIT: Technology Review, 9, April 2012), available at: http://www.technologyreview.com/communications/40075/?p1=A1

531 see Honan, Mathew. "I Am Here: One Man's Experiment With the Location-Aware Lifestyle" (Wired Magazine, 19 January 2008), available at: http://www.wired.com/gadgets/wireless/magazine/17-02/lp_guineapig

532 The Garmin-Asus' Nüvifone G60, for instance, had also planned to put location-awareness as an integral part of its capabilities, whereby location information provided by GPS is integrated into everything, from emails, text messages and photos to social networking and even gaming

533 see Joey Hess' explanation, available at: http://kitenet.net/~joey/blog/entry/Palm_Pre_privacy/

534 The security analyst Samy Kamkar recently discovered that Google's HTC Android smartphone collected its location every few seconds and directly transmitted the location data, including a unique phone identifier, to Google several times an hour. see Angwin, Julia., Jennifer Valentino-Devries. "Apple, Google Collect User Data" (Wall Street Journal, Technology, 22 April 2011).

ers of web browsers are now more and more ensuring that their software supports both location-aware web-based applications and location-aware web browsing. Mozilla's Firefox now enables web applications to automatically know where the user is located, which will, for example, provide local search results without the need to include a post-code in the search query.

People are more and more revealing what they are currently doing via Twitter, what is currently on their mind via Facebook, and what they are currently working on via LinkedIn. Now, letting people, or the world for that matter, know where you are precisely continuously in real-time is increasingly becoming popular. This popularity will likely only increase, since Twitter has integrated location data into 'tweets' through geo-tagging, whereby location information can automatically be annotated to a person's tweets, and Facebook has also announced that it plans to integrate location-based features.

There are already now a multitude of dedicated location-aware applications, which enable users to reveal exactly where they are in real-time. These applications, which operate on GPS-equipped smartphones and tablet PCs, are changing our daily lives. As Mathew Honan explains, "[t]his one input – our coordinates – has the potential to change all the outputs. Where we shop, who we talk to, what we read, what we search for, where we go – they all change once we merge location and the Web".[535] In addition to the LBS available on smartphones, there are other services, systems or devices that are capable of collecting and subsequently retaining location information, such as intelligent transportation systems (ITS) and automatic license plate recognition (ALPR) or automotive number plate recognition (ANPR) systems. However, while many of the location-aware applications on smartphones, for example, simply enable location-relevant searches, such as nearby restaurants and venues,[536] a number of these applications are in fact focused on keeping track of the movements of individuals.

LifeAware not only tracks you via your smartphone, it also allows you to connect with other people running the application on their smartphones, showing you their current location.[537] *Loopt* provides a service, whereby users can discover where their friends are located and even what they are doing via detailed, interactive maps on their

535 see Honan, Mathew. "I Am Here: One Man's Experiment With the Location-Aware Lifestyle" (Wired Magazine, 19 January 2008), available at: http://www.wired.com/gadgets/wireless/magazine/17-02/lp_guineapig

536 see Biba, Erin. "Inside the GPS Revolution: 10 Applications That Make the Most of Location" (Wired Magazine, 19 January 2008), available at: http://www.wired.com/gadgets/wireless/magazine/17-02/lp_10coolapps?currentPage=3

537 LifeAware, available at: http://www.lifeaware.net/

smartphones.[538] *Highlig.ht* and *Ban.jo* alert users when their (Facebook) friends are nearby. *Sonar*[539] also determines if any friends (or friends of friends) are close by based on a user's Facebook networks. *Sniff* lets users instantly locate their friends anywhere in real-time using their smartphone. *Glancee* even lets you know when other people with similar interests are nearby. *WhosHere also* enables users to locate people in real-time that match their profile anywhere in the world. Other location-based services include *Foursquare* and the location-based social network websites *Whrrl*[540] *and BrightKite.*[541] Another smartphone application called *Glympse* enables users to broadcast where they are in real-time. GTX Corp. has developed an iPhone application called *LOCiMe*, which converts the smartphone into a 2-way GPS receiver, allowing users to locate their friends and transmit their location to others.

Google has also launched *Latitude*, free software that enables people to always keep track of each other using their smartphones. *Latitude* could potentially be used as a tool, for example, by parents to keep tabs on their children's' location. However, it can be used by anyone to find anyone else, assuming permission is given.[542] On the other hand, *Latitude,* like *Loopt,* apparently does not keep a log of the real-time location data. On the other hand, *Latitude* is set by default as a website with authorization to Gmail accounts. The latest addition to Google's *Latitude* is the "Public Location Badge", which enables users to share their location on their blog or website, but without the ability to limit who will be able to access this location information, since it will be publicly available to everyone with access to the Internet.

Furthermore, Sprint launched the Business Mobility Framework,[543] which allows employers to track employees, and other companies have also launched similar systems. It is already common for GPS to be used to track certain categories of employees in their vehicles, such as taxi drivers[544] and contractors, whether they like it or not, and

538 Loopt, available at: http://www.loopt.com/

539 Sonar, available at: http://sonar.me

540 Whrrl, available at: http://www.whrrl.com/

541 Brightkite, available at: http://brightkite.com/

542 Google Mobile, available at: http://googlemobile.blogspot.com/2009/02/locate-your-friends-in-real-time-with.html

543 Sprint, available at: http://www.sprint.com/business/products/products/bmf.html

544 see Karni, Annie. "GPS Concerns Taxi Drivers" (New York Sun, 5 January 2007), available at: http://www.nysun.com/new-york/gps-concerns-taxi-drivers/46133/

the law does little to prohibit this activity. RFID is also already increasingly being used to register the comings and goings of employees at their place of work.

However, unlike the LBS or location-aware applications available on smartphones, the location information generated by HIMs, at present, may be more difficult for implantees to manage. For example, HIMs make it impossible to falsify one's location and smartphones do not normally broadcast an individual's identity, unlike RFID implants. Smartphones can simply be left at home or the LBS on smartphones can be deactivated. In addition, most smartphones, at least for now, normally do not constantly transmit their location.

7.4 POTENTIAL SECURITY AND WELL-BEING BENEFITS

The common good of public security and security of critical infrastructure, in addition to the other benefits, which HIMs could help to enhance, is perhaps why people might be open to their widespread deployment. There are indeed various legitimate non-medical uses of HIMs, ranging from identifying employees at secure facilities to locating a missing child and tracking criminals.

The occurrence of child abductions every year in the US is disturbing,[545] while the number of involuntary missing children is daunting.[546] This has led some parents and RFID/GPS profiteers, such as VeriChip/ADS, to suggest implanting HIMs in children. Indeed, if an abducted child had been implanted with a RFID implant, his or her

[545] On the other hand, Frank Furedi argues that the fear of parents over their child being kidnapped is not justified by the figures and that this fear is mostly hyped by the media (2006, p. 32). However, according to a 2002 report by the U.S. Department of Justice, in 1999 there were an estimated 33,000 nonfamily child abductions and 115 child abductions of the stereotypical type in the US. "A nonfamily abduction occurs when a nonfamily perpetrator takes a child by the use of physical force or threat of bodily harm or detains a child for at least 1 hour in an isolated place by the use of physical force or threat of bodily harm without lawful authority or parental permission; or when a child who is younger than 15 years old or is mentally incompetent, without lawful authority or parental permission, is taken or detained by or voluntarily accompanies a nonfamily perpetrator who conceals the child's whereabouts, demands ransom, or expresses the intention to keep the child permanently." "Stereotypical kidnappings are the particular type of nonfamily abduction that receives the most media attention and involves a stranger or slight acquaintance who detains the child overnight, transports the child at least 50 miles, holds the child for ransom, abducts the child with intent to keep the child permanently, or kills the child. They represent an extremely small portion of all missing children". see Sedlak, Andrea J., et al. "National Estimates of Missing Children: An Overview" in *National Incidence Studies of Missing, Abducted, Runaway, and Thrownaway Children*. (Office of Juvenile Justice and Delinquency Prevention, Office of Justice Programs, U.S. Department of Justice, October 2002), pp. 4-7, available at: http://www.ncjrs.gov/pdffiles1/ojjdp/196465.pdf

[546] However, nearly a third of all missing children have benign explanations, but account for many of the reported cases to the police. see Ibid., p. 6.

location could be determined if the child comes near to a RFID reader linked to the Internet.[547] However, RFID implants could be potentially destroyed using microwaves or obstructed by covering the implantee's arm with metal. In extreme cases, the implantee's arm or hand could either be cut off or his or her captors could simply carve the HIM out.[548]

On the other hand, if a child implanted with a GPS implant was kidnapped or abducted, his or her exact, real-time location could be provided without delay to the police and enable AMBER Alerts distributed via text messages based on the physical location of subscribers determined via their smartphone or their own HIM, informing people that a child of a certain description has gone missing in their vicinity or is located in their vicinity. This is especially important since experience has shown that an abducted child's chance of survival dramatically decreases after the first day, and so the ability to locate the kidnapped child immediately is crucial. However, since nearly all reported cases of missing children have benign explanations,[549] the ability of parents to immediately and easily locate their children through GPS via the Internet could, in theory, reduce avoidable emergency calls. Additionally, if a child implanted with a GPS implant were to become lost, for example, in a forest, a search and rescue team would effortlessly be able to locate him or her.

But, even the GPS signal received by GPS implants can be 'spoofed', as demonstrated by researchers at Cornell University, who spent more than one year building equipment that can transmit fake GPS signals capable of fooling receivers.[550] This would result in transmitting the wrong signal to the implant and inaccurate location information to the HIM service provider, rendering the GPS implant not very helpful to the implantee if he/she indeed needed to be located as a consequence of being kidnapped or of becoming involuntary lost or missing. GPS signals can also be potentially 'jammed' using commercially available jamming devices.

---

547 Solusat, the Mexican distributor of the VeriChip, is marketing the device as an emergency ID tag called VeriKid. see Scheeres, Julia. "Tracking Junior With a Microchip" (Wired News, 10 October 2003), available at: http://www.wired.com/science/discoveries/news/2003/10/60771

548 Perhaps, even a child wearing something which states, "I have an implant" could have the similar deterrent effect that signs placed in homes stating "Beware of Dog" or other home security warning stickers may have.

549 see Sedlak, Andrea J., et al. "National Estimates of Missing Children: An Overview" in *National Incidence Studies of Missing, Abducted, Runaway, and Thrownaway Children*. (Office of Juvenile Justice and Delinquency Prevention, Office of Justice Programs, U.S. Department of Justice, October 2002), available at: http://www.ncjrs.gov/pdffiles1/ojjdp/196465.pdf

550 Ju, Anne. "Researchers raise uncomfortable questions by showing how GPS navigation devices can be duped" (Cornell Chronicle, 19 September 2008), available at: http://www.news.cornell.edu/stories/Sept08/GPSSpoofing.aj.html

HIMs can also provide a secure form of identification, but this is debatable (see Section 7.5 for further discussion). Unlike conventional forms of identification, such as ID cards or passports, HIMs cannot be lost or stolen. RFID implants, for example, could be used to verify the identity of a person before granting their entry into secure sites, such as nuclear facilities. RFID implants and the strategic deployment of fixed and mobile RFID readers can theoretically provide companies or government agencies with the ability to both unmistakably identify employees and track their comings and goings and other movements. This is especially important in restricted access areas, such as nuclear facilities and luggage sorting halls at airports, where physical access technology plays a crucial role. RFID implants in this context could play a significant role in national security.

HIMs can also provide an extra layer of banking security, whereby an ATM machine or a bank teller can authenticate the identity of a customer by using a RFID reader. As such, if the data stored on HIMs is secure, HIMs can help to prevent fraud and identify theft. Equally, PCs could come equipped with RFID readers which are then able to authenticate a user via his or her implant, adding yet another layer of security to Internet banking or e-commerce. Already, there are computers that come equipped with fingerprint biometric scanners and software.

HIMs could also be used in 'smart gun' technology. In April 2004, ADS announced a partnership with gun manufacturer FN Manufacturing to produce a prototype of a gun that can only be fired if operated by their owner identified with a RFID tag implanted in his or her hand.[551] The concept behind the prototype is that a RFID reader in the gun reads the HIM's unique identification number and sends a digital signal unlocking the trigger so it can be fired. If the person who handles the gun does not have a HIM or the RFID reader does not recognize a HIM's unique ID number, then the gun will remain locked.

Prisoners convicted of violent crimes could be implanted with RFID microchips to actively track their movements within prisons or with GPS implants to immediately locate them if they happen to escape prison. Parolees of violent crimes could also be implanted with RFID/GPS implants to either actively or passively track or monitor their movements and whereabouts, in order for a law enforcement agency to be immediately notified of an offenders' growing proximity to the stored addresses of the victims of their previous crimes.

HIMs implanted into convicted pedophiles/sex offenders could help to better keep track of their location or monitor their movements in real-time, regardless if they are

551 see "No Chip in Arm, No Shot From Gun" (Associated Press, 14 April 2004), available at: http://www.wired.com/science/discoveries/news/2004/04/63066

registered or not in compliance with Megan's Law.[552] An application called Offender Locator, for example, is available on the iPhone, which displays the names, addresses, faces and criminal records of registered sex offenders near the user's location in real-time via the iPhone's GPS capability.

The location information generated by HIMs, let alone smartphones, will surely be useful to the continued development of the Information Sharing Environment (ISE), which aims to combine or "fuse" information controlled by all levels of government, including information held by the private sector, for subsequent analysis in the fight against terrorism.[553] In fact, the Executive Summary of the Fusion Center Guidelines, developed by the Department of Justice, recommends at minimum the attainment of access to location information. Governmental access to location information maintained by the private sector is yet another example of the cooperation between the US Government and the private sector in collecting and storing data within the emerging security-industrial complex that Robert O'Harrow (2005) warns us about in *No Place to Hide*.

Finally, RFID technology, whereby tiny RFID microchips are covertly tagged (or even implanted) onto targeted individuals (terrorists), could also be potentially used to locate and track the targeted individuals for termination by way of UAVs. However, these RFID tags are far more advanced than the current RFID implants discussed here. These capabilities are reportedly being developed and demonstrated by the US military, as part of the GWOT, and are purportedly just one component of the classified "Clandestine Tagging, Tracking, and Locating" (CTTL) program.[554]

7.5 SECURITY RISKS AND DRAWBACKS

While HIMs offer a number of security benefits, even if most are currently hypothetical, many of the security risks and drawbacks of HIMs, and the associated technology of RFID and GPS, are serious and real. The security benefits of HIMs could be compromised, if these security risks and drawbacks are not dealt with accordingly.

552 Megan's Law is the name given to the laws in the US requiring law enforcement authorities to make information available to the public regarding registered sex offenders. At the Federal level, the Sexual Offender (Jacob Wetterling) Act of 1994 requires convicted child sex offenders or pedophiles to notify local law enforcement agencies of any change of address after being released from prison. This information is publicly available.

553 The 9/11 Commission Act focused on establishing the Homeland Security Department's fusion center program.

554 see Weinberger, Sharon. "What is Woodward's Secret Weapon in Iraq?" (Wired, 9 September 2008), available at: http://www.wired.com/dangerroom/2008/09/whats-the-milit/

As the Data Privacy and Integrity Advisory Committee of the Department of Homeland Security (DHS) affirmed, "[a]ttempts to improve speed and efficiency through using RFID to track individuals raise important privacy and information security issues".[555] The US GAO observed, with regards to RFID microchips embedded in passports (ePassports) and ID cards, in a report titled *Information Security: Radio Frequency Identification Technology in the Federal Government* [hereinafter called "GAO RFID Report"], that "[w]ithout effective security controls, data on the tag can be read by any compliant reader; data transmitted through the air can be intercepted and read by unauthorized devices; and data stored in the databases can be accessed by unauthorized users".[556] Moreover, in a staff report on RFID, the FTC points out, "security concerns are likely to arise in connection with interoperable tags, which can be read by different enterprises sharing information associated with those tags".[557]

IT security experts have been warning about the security risks of RFID tags for some time now, and even have demonstrated those risks. 'Ethical hacker' Chris Paget has famously demonstrated using a low-cost RFID reader that he could surreptitiously read and clone the EPC Generation 2 RFID tags embedded in US passport cards (not to be confused with US ePassports) and Enhanced Driver's Licenses. *The Hacker's Choice*, a group of international experts on computer security, provided an emulator applet for copying ePassports and demonstrated their considerable security loopholes.[558]

The VeriChip RFID implant is based on ISO 11784/85, the same international standard that regulates animal-implantable RFID microchips. However, ISO 11784/85 is not well-known for ensuring the security and integrity of the data held on the microchips. Identity theft via RFID implants is especially a grave (data) security concern.[559]

---

[555] The Use of RFID for Human Identification: A Draft Report from DHS Emerging Applications and Technology Subcommittee to the Full Data Privacy and Integrity Advisory Committee, Version 1.0, p. 3, available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_rpt_rfid_draft.pdf
(This precise statement was removed from the final adopted version of the report)

[556] Information Security: Radio Frequency Identification Technology in the Federal Government, The United States Government Accounting Office, May 2005, p. 19, available at: http://www.gao.gov/new.items/d05551.pdf

[557] FTC staff report on RFID, p. 16.

[558] see *The Hacker's Choice* explanation, available at: http://freeworld.thc.org/thc-epassport/

[559] Identity theft is already the most significant consumer complaint. For instance, during 2009, identity theft was by far the number 1 consumer complaint, accounting for 21% of all consumer complaints in the US. see the 2009 Consumer Sentinel Network Data Book, Federal Trade Commission, February 2010.

As demonstrated by Annalee Newitz and Jonathan Westhues,[560] VeriChip's RFID implant, which have no adequate security features, can be 'cloned'.[561] Directions on how to do so were made available on the Internet.[562] Jonathan Westhues also explained on his website about another vulnerability of VeriChip's implant using another type of attack called a "replay attack", which refers to when an attacker replays an earlier transmitted unique identification number.[563] Researchers from John Hopkins University and RSA Laboratories also demonstrated that the data on an RFID tag can be stolen by reading the tag's signal, then 'cracking' the tag's encryption key and creating a 'clone' of the RFID tag. The tag used even had a 40-bit encryption key.[564] A group of doctors from the American Medical Informatics Association equally recognized that VeriChip's RFID implant is vulnerable to attacks.[565] Thus, RFID implants are currently vulnerable because the microchips can be cloned or spoofed, especially if the implant is based on inadequate standards.

The hosts of *Mythbusters,* a popular TV show produced by the Discovery Channel, wanted to demonstrate in an episode segment "how hackable, how reliable, how trackable" are RFID microchips. VISA, MasterCard and American Express, which all have a certain interest in using RFID for contactless payment, apparently pressured the Discovery Channel to refrain from airing this episode.[566] In the end, the show pursued a different topic during their episode on RFID.

Furthermore, a group of computer experts from Vrije Universiteit demonstrated that it is also possible to transmit a virus or malware software onto RFID tags, causing

---

560 Fulton, Nic. "High-tech cloning" (Reuters, 22 July 2006), available at: http://blogs.reuters.com/blog/2006/07/22/high-tech-cloning/

561 The act of 'cloning' a RFID tag, also known as 'spoofing', is similar to the way credit cards can be copied, known as 'skimming', whereby an account number and other data needed to clone a credit card is covertly copied. But, RFID tags do not need to be physically taken, in order to be copied.

562 see Jonathan Westhues' website, available at: http://cq.cx/verichip.pl

563 *Ibid.*

564 see Bono, Steve., et al. *Security analysis of a cryptographically-enabled RFID device*, USENIX Security Symposium Proceedings of the 14th conference on USENIX Security Symposium, Volume 14, 2005.

565 see Halamka, John., et al. The Security Implications of VeriChip Cloning (Journal of the American Medical Informatics Association, Volume 13, Issue 6, 2006), pp. 601-607.

566 see Leyden, John. "*Mythbusters* RFID episode axed after 'pressure' from credit card firms", The Register, 3 September 2008, available at: http://www.theregister.co.uk/2008/09/03/mythbusters_gagged/

unwanted actions to occur and jeopardizing the databases linked to the tags.[567] Any RFID system, which transmits information over the Internet, is equally subject to cyber attacks, and many of the same security dilemmas of RFID microchips are, accordingly, relevant to RFID implants. Therefore, RFID implants and the creation of an 'Internet of Persons' could add a new dimension to cybercrime or hi-tech crime, now one of the leading criminal activities, whereby human bodies themselves, as opposed to just computers, become the target of cybercriminals and vulnerable to a cyber attack. As a result, it is conceivable that HIMs and, therefore, human beings themselves, in a way, could be infected with a virus or malware software and that a computer virus pandemic caused by RFID implants is a possibility.[568] Indeed, Mark Gasson, a scientist at the University of Reading, became the first human to be infected with a computer virus by infecting his RFID implant. Gasson is also currently researching the potential risks associated with other electronic devices implanted into humans, in addition to RFID implants, such as cochlear implants and pacemakers.[569] Sandler et al. (2010) have equally raised their concerns over the security vulnerabilities of the software code of (wireless) implantable medical devices.[570]

The RFID microchips, however, are not the only vulnerability of the system. The middleware/software and associated databases are also subject to security risks. The Food and Drug Administration (FDA) cites, one of the potential risks associated with the VeriChip's RFID implant, are "compromised information security".[571] Although an implant's ID number is essentially just a number and basically inconsequential without additional access to the integrated database(s), there is the threat that a hacker or an unauthorized third party, other than the implantee or authorized data controller, could indeed gain access to the associated data. Therefore, another major security threat to the implantee is the potential for unauthorized access to his/her electronic health data,

---

567 Rieback, M.R., et al. *RFID Viruses and Worms* (Department of Computer Science, Vrije Universiteit Amsterdam, 2006), available at: http://www.rfidvirus.org

568 Interestingly, I wrote about this possibility at least a year before the news broke on unique Mark Gasson's research project.

569 see Palmer, Maija. "Scientist 'infects himself' with computer virus", (Financial Times, 26 May, 2010), available at: http://www.ft.com/cms/s/0/2e2f5ea4-68b5-11df-96f1-00144feab49a.html

570 Equally, any software-controlled, wireless medical device could be vulnerable.
see, e.g., Darlene, Storm. "Feds pressed to protect wireless medical devices from hackers" (ComputerWorld, 11 April 2012), available at: http://blogs.computerworld.com/20015/feds_pressed_to_protect_wireless_medical_devices_from_hackers?source=rss_blogs

571 Federal Register, Volume 69, Number 237, 10 December 2004, pp. 71702-71704.

location information or any other personal information associated with the HIM and stored on the multiple associated databases.

Other security concerns pertain to the contactless nature and non-direct line-of-sight capability of RFID technology. As a result, RFID normally operates unnoticeably, making it difficult if not impossible for people to know when they are being identified and/or tracked.[572] Without strong security standards, the information contained on HIMs can therefore be read without the implantee's knowledge or consent, leaving RFID implantees considerably deprived of the ability to control the information others may know about them.

With regards to the security drawbacks of prospective GPS implants, relying too much on GPS to track and monitor the movements of parolees of violent crimes and sex offenders could result in providing a false sense of security for society as a whole, as some have pointed out.[573] GPS tracking is certainly not a silver bullet for preventing crime, as was shown with the murder of 13-year-old Alycia Nipp by a sex offender who was under monitoring via a GPS bracelet.[574] But, this particular sex offender was under passive monitoring, as opposed to active monitoring. Nevertheless, the sex offender or parolee could simply become unconcerned that he is being monitored and commit another crime regardless.

Paradoxically, as easily as an implantee can be found by law enforcement agencies, if he or she were to be kidnapped or was to become lost, criminals could also intentionally locate an implantee. The availability of location information, for instance, could lead to a stalker somehow accessing that information, if adequate safeguards are not put in place. As the National Network to End Domestic Violence (NNEDV) warns, RFID can be used by abusers to track or stalk their victims.[575] The same is obviously true and even worse for GPS and just about any location-based service.

572 see The Use of RFID for Human Identify Verification, Report No. 2006-02, Data Privacy & Integrity Advisory Committee, Adopted 6 December 2006, available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf

573 see McLaughlin, Eliott C. and Patrick Oppmann. "Sex offender kills teen while under GPS monitoring, police say" (CNN.com, 12 March 2009) available at: http://edition.cnn.com/2009/CRIME/03/12/sex.offender.gps/index.html

574 Ibid.

575 see a paper prepared by the NNEDV, available at: http://www.aclunc.org/issues/technology/asset_upload_file364_7757.pdf

7.6 SCOPE OF DEPLOYMENT

7.6.1 Actual deployment in the US

The research that led to the development of RFID occurred decades ago, however, the innovation steps that have translated the research and development into various marketable products and solutions, such as access control cards and identity cards, and services for supply chain management, is relatively recent. HIMs are just one of the latest innovation concepts developed using RFID technology.

HIMs are not theoretical or science fiction, they are real and here. The concerns over the deployment of HIMs are not premature. The deployment of HIMs is indeed spreading, however, just not as much as some proponents may like.

VeriChip's[576] previously publicly stated goals of implanting millions of Americans with their implantable RFID tags, has so far not been successful. As of 17 March 2008, 616 people have had VeriChip's RFID implant implanted.[577] But, this number is likely higher when including those who have been implanted outside the US. Moreover, this number does not include the number of people who have implanted an implantable RFID tag/microchip independent of VeriChip (see below for further explanation).

VeriChip had focused on targeting people with medical conditions, such as diabetes and Alzheimer's disease or dementia, and senior citizens. As part of a study on the VeriMed Patient Identification System, VeriChip implanted their RFID implants in 200 individuals suffering from Alzheimer's disease and other forms of dementia, as well as their caregivers.[578] A number of diabetics have also been implanted. In addition, VeriChip equipped a large bus as a mobile "chipping station", also known as the

---

[576] In 2009, VeriChip Corporation changed its name to PositiveID Corporation after completing its acquisition of Steel Vault Corporation. Throughout this dissertation, however, the company will still be known as VeriChip to avoid confusion. Nevertheless, the new company still markets their RFID implant (VeriChip), but has also now taken the "capabilities of RFID implantable microchips beyond simple identification" to create the "GlucoChip", which "combines an embedded bio-sensor system on an implanted RFID microchip". "One potential application of this bio-sensor system is an implantable, bio-sensing RFID microchip that measures glucose levels in the body in real time". Further information is available at: http://www.positiveidcorp.com/products_glucochip.html

[577] see VeriChip Corp.'s 10-K Annual Report for the fiscal year ended 31 December 2007, p. 13, available at: http://www.sec.gov/Archives/edgar/data/1347022/000136231008001657/c72788e10vk.htm

[578] see VeriChip Corp., Press Release, 22 February 2003, "VeriChip Corporation Partners with Alzheimer's Community Care to Conduct Study of VeriMed Patient Identification System", available at: http://www.verichipcorp.com/news/1172151146

"chip mobile".[579] As of 31 December 2007, more than 200 hospitals and other medical facilities have adopted the VeriMed Patient Identification System protocol in their emergency rooms and have become a part of the network.[580]

During the Hurricane Katrina disaster relief, US Disaster Mortuary Operational Response Team (DMORT) and health officials in Mississippi's Harrison County implanted RFID implants, donated by VeriChip, to speed up or facilitate the process of identifying corpses.[581] The system is now marketed as VeriTrace. In 2007, VeriChip reportedly managed to convince the State of Georgia to buy a package of the company's VeriTrace system which consisted of 500 RFID implants, 5 customized Ricoh 500SE digital cameras capable of receiving both RFID and GPS data wirelessly and adding geographical identification metadata (or GPS coordinates) to the image (known as geotagging), 5 VeriTrace Bluetooth handheld readers, and a web-enabled database. The system can identify, track and automatically record each implant's ID number along with the GPS coordinates captured by the Ricoh cameras embedded in the images, which enables the precise cataloging of all data and images related to human remains after a disaster.[582]

In February 2006, RFID implants were also infamously implanted in employees at CityWatcher.com, a company in Cincinnati, Ohio, with the help of Six Sigma Security, to establish an access control system at the company's secure data center.[583] Although it was not exactly a condition of employment, it would have been difficult for some employees to work there meaningfully without a HIM.

Nevertheless, the objective of privacy advocates to put VeriChip Corp. out of business might in fact one day materialize. VeriChip Corp.'s implant business has yet to generate a viable profit for the company (as of 2009), while the company's future is

579 see VeriChip's FAQ webpage, available at: http://www.verichipcorp.com/content/company/corporatefaq

580 see VeriChip Corp.'s 10-K Annual Report for the fiscal year ended 31 December 2007, p. 13, available at: http://www.sec.gov/Archives/edgar/data/1347022/000136231008001657/c72788e10vk.htm

581 see Kanellos, Michael. "RFID chips used to track dead after Katrina" (*CNET News*, 16 September 2005), available at: http://www.news.com/RFID-chips-used-to-track-dead-after-Katrina/2100-11390_3-5869708.html?tag=nw.2;
RFID implants were also implanted in the bodies of victims of the Tsunami in Thailand. see Meyer, H.J., et al. *Implantation of radio frequency identification device (RFID) microchip in disaster victim identification (DVI)*. (Forensic Science International, Volume 157, Issue 2, 2006), pp. 168-71.

582 see VeriChip Corp., Press Release, available at: http://www.businesswire.com/news/google/20070509005155/en

583 see "US group implants electronic tags in workers" (Financial Times, 12 February 2006), available at: http://www.ft.com/cms/s/ec414700-9bf4-11da-8baa-0000779e2340.html

still in doubt. But, the potential privacy threat of HIMs will persist, regardless of the existence of VeriChip Corp.

Although VeriChip Corp. is the only official or FDA approved provider of human implantable RFID tags, going through VeriChip Corp. is not the only way of getting a HIM implanted. VeriChip Corp. does not have a patent or monopoly on glass encapsulated RFID tags. There are a number of other glass encapsulated RFID tag manufacturers and distributors, such as Trovan, Destron Fearing (a subsidiary of Digital Angel[584]) and Philips. Only that these glass encapsulated RFID tags are not marketed, promoted or approved for human implantation, but rather for implantation in animals. Nonetheless, any small, glass encapsulated RFID tag could easily be bought and used for human implantation.

This is indeed what is actually occurring. These so-called "guerrilla taggers" are the latest pioneers of a "brave new world", having RFID implants implanted in the less conventional way. Amal Graafstra is one of the more well-known. He chose not to go through VeriChip because it uses a proprietary system and he also did not want to sign up for the global VeriChip subscriber registry. He has two RFID implants, one in each hand. His left hand contains a 3mm x 13mm EM4102 type glass RFID Ampoule tag that was implanted by a cosmetic surgeon. His right hand contains a 2mm x 12mm Philips HITAG 2048 S implant with crypto-security features and 255 bytes of read-write memory storage space. It was implanted by a family doctor using an Avid injector kit just like the ones used on pets. Graafstra's development is an example of user-driven innovation (UDI). He has developed the means to access his front door, car door, and log into his computer using his RFID implants, and has written a book called *RFID Toys*, which details how to develop these and other RFID-enabled projects. Explanations, pictures and videos can be downloaded from his website.[585] There are numerous other guerrilla taggers (perhaps hundreds) around the world who have also engaged in do-it-yourself RFID implantation. Nancy Nisbet, a Canadian artist, is another well-known guerrilla tagger. Of course, they are all copycats of Kevin Warwick, the renown Professor of Cybernetics at the University of Reading and author of *I Cyborg*,[586] who had a RFID chip implanted in 1998 (later removed) allowing him to automatically open doors

---

[584] The current President and CEO of Digital Angel Corporation, Joseph J. Grillo, has extensive experience in identification and tracking technology. He was formerly the President and CEO of the Global Technologies Division of Assa Abloy, and before that managed the Identification Technology business unit of Assa Abloy. Before that, he was President of HID.

[585] see Amal Graafstra's website, available at: http://amal.net/rfid.html

[586] Warwick, Kevin. I *Cyborg* (Century, 2002).

and turn on lights, and four years later a micro electrode array surgically implanted into the median nerve fibers of his left arm allowing him to be connected to the Internet and control a robotic arm from afar.

The development of the GPS implant, on the other hand, is still most likely in its near final stages of development and miniaturization, according to ADS, which apparently had successfully tested a working prototype several years ago,[587] consistent with the company's previous public statements made repeatedly that it intended on developing a HIM with GPS tracking capabilities. ADS/Digital Angel, formerly the largest shareholder of VeriChip Corp., is the most notable company publicly involved in the R&D of GPS implants and acquired the rights to U.S. Patent No. 5,629,678 in 1999.[588] But, a GPS implant has yet to hit the consumer market, and ADS/Digital Angel has since removed this information from the Internet and altered its website and apparently its business plan.[589] A patent application for a GPS implant for animals was filed with the U.S. Patent Office.[590] The patent application cites the technology used in the GPS implant apparently developed by ADS/Digital Angel.[591] Nonetheless, it is perhaps not incredibly farfetched to assume that national intelligence agencies or secret government-funded research projects are or were also working to develop GPS implants or may have already done so. Though, there is no publicly available proof to this statement.

Nevertheless, the technology, however, is not really the obstacle to the widespread deployment of HIMs, whether RFID or GPS-based, and nor is the law for that matter. The difficulties VeriChip Corp. and ADS have faced, for instance, and the obstacles to the

---

[587] see Applied Digital Solutions Inc., Press Release, 13 May 2003, "Applied Digital Solutions Announces Working Prototype of Subdermal GPS Personal Location Device", available at: http://findarticles.com/p/articles/mi_m0EIN/is_2003_May_13/ai_101629083

[588] see Applied Digital Solutions, Inc., Press Release, 15 December 1999, "APPLIED DIGITAL SOLUTIONS ACQUIRES RIGHTS TO WORLD'S FIRST DIGITAL DEVICE - IMPLANTABLE IN HUMANS - WITH APPLICATIONS IN E-BUSINESS TO BUSINESS SECURITY, HEALTH CARE AND CRIMINAL JUSTICE" (retrieved through Internet Archive's Wayback Machine), available at: http://web.archive.org/web/20000511001424/www.digitalangel.net/pr_12_15_99.htm

[589] This information, nonetheless, can also be retrieved through the use of Internet Archive's Wayback Machine. see, for instance, Digital Angel's website dated July 11, 2000, available at: http://web.archive.org/web/20000711033923/http://www.digitalangel.net/

[590] see U.S. Patent Application No. 20090009388, filed by Carole A. Wangrud on 8 January 2009, which claims to be a system for monitoring and tracking the location of animals comprising of a GPS implant designed to be transplanted subcutaneously.

[591] *Ibid.*, para. 0025.

widespread deployment of HIMs pertain rather to the uneasiness of the public towards HIMs. As VeriChip Corp. notes in its 2007 10-K report, privacy concerns and negative media coverage are significant risks to its business, acknowledging that people may not be willing to be implanted and that physicians may be reluctant to recommend the procedure.[592] Other obstacles include the fact that VeriChip's RFID implant costs around $200 and is not covered by private healthcare insurance companies or by Medicare/Medicaid.

The perception of the public towards HIMs and their effects might slowly change. We are already seeing the general acceptance of the deployment of numerous other tracking technologies, devices, applications and schemes, many of which have similar effects (see sections 7.3.6 and 7.7). HIMs are arguably just the next step.

7.6.2 Potential deployment

The potential greater (or perhaps widespread) deployment of HIMs is arguably not farfetched. On the basis that the implantation of HIMs is cheap and quick and that the technology is already in place, the futurist Matthew Sollenberger predicted in 2007 that "[t]here is at least a low probability of chipping becoming widespread within 10 years".[593] Wolfgang Grulke, a former IBM executive, winner of the prestigious IBM Outstanding Innovation Award and Chairman of FutureWorld International, has equally predicted that HIMs will be common in a decade or so. As a report of the consortium of the SWAMI project[594] agrees,

> [i]ndeed, it is not impossible to imagine a day when almost everyone will have implantable devices, not only for tracking their whereabouts, but also for monitoring their physiological condition. At the same time, there may be considerable social pressure, perhaps even legal requirements, for individuals to bear

---

592 see VeriChip Corp.'s 10-K Annual Report for the fiscal year ended 31 December 2007, pp. 34-35, available at: http://www.sec.gov/Archives/edgar/data/1347022/000136231008001657/c72788e10vk.htm

593 Sollenberger, Matthew. "Chipping People" (Social Technologies, 12 November 2007), available at: http://www.socialtechnologies.com/FileView.aspx?fileName=PressRelease11122007.pdf

594 The SWAMI (Safeguards in a World of Ambient Intelligence) project aimed to provide an overview of the key social, legal and ethical implications of ambient intelligence and highlight the privacy threats.

> such implants as a security measure. One could further foresee such implants interacting with the "intelligence"-embedded, networked environment too.[595]

More recently, in a roadmap on current and future trends, Richard Watson included as a possibility that by 2025-2035 all babies born will be implanted with GPS and ID chips.[596]

Kevin Haggerty, an expert on surveillance and Professor of Sociology, wrote an article in the Toronto Star explaining evocatively how this could develop in the US.[597] Haggerty describes a scenario whereby the Government starts off implanting stigmatized groups, such as pedophiles or sex offenders and criminals, and then suggests that illegal aliens and soldiers be implanted, until eventually a majority of Americans become implanted for one reason or another. As Haggerty asserts, it is "[b]est to contemplate these dystopian potentials before we proffer the tender forearms of our sons and daughters".[598]

In other words, there is a likelihood that the mandatory implantation of HIMs for sex offenders and parolees of violent crimes for public security purposes will not cause most people to speak up in protest. Then, the mandatory implantation of HIMs in soldiers for their safety will likely not cause uproar from private citizens. Then, the mandatory implantation of HIMs in employees at secure facilities, such as nuclear power plants, again for the sake of public security, will likely make sense to many people, especially those who do not work at these facilities. As the mandatory implantation progresses with additional justifications, more and more people will be implanted with a HIM until there are few categories of people leftover that do not meet the requirements for mandatory implantation.[599]

---

595 Friedewald, M., R. Lindner & D. Wright (eds.), "Policy Options to Counteract Threats and Vulnerabilities in Ambient Intelligence", SWAMI Deliverable D3: A report of the SWAMI consortium to the European Commission under contract 006507, June 2006, (Draft version), p. 37, available at: http://www.isi.fhg.de/publ/downloads/isi06b24/SWAMI_D3_030706.pdf

596 see Trends & Technology Timeline 2010+ , available at: http://nowandnext.com/PDF/trends_and_technology_timeline_2010.pdf

597 see Haggerty, Kevin. "One generation is all they need" (The Star, 10 December 2006), available at: http://www.thestar.com/sciencetech/article/136744

598 *Ibid*.

599 *Ibid.*

Therefore, the famous words of Friedrich Gustav Emil Martin Niemöller may be relevant here for the potential deployment of HIMs. In speeches and in a poem, referring to the Nazis, the German pastor and theologian famously states:

> In Germany, they first came for the communists, and I didn't speak up because I wasn't a communist. Then they came for the Jews, and I didn't speak up because I wasn't a Jew. Then they came for the trade unionists, and I didn't speak up because I wasn't a trade unionist. Then they came for the Catholics and I didn't speak up because I wasn't a Catholic. Then they came for me – and by that time there was nobody left to speak up.

If RFID does become the primary method of identification, human beings will then commonly be electronically identified for verification purposes. For reasons of homeland security, RFID tags are already being embedded in US passports, enhanced state driver's licenses and ID cards, and in the Western Hemisphere Travel Initiative (WHTI) cards. RFID implants are naturally the next step in electronic identification (eID). Dr. Richard Seelig, formerly VP for Medical Affairs at VeriChip, similarly advocated that RFID implants "could function as a theft-proof, counterfeit-proof ID, like having a driver's license embedded under your skin".[600] RFID implants could thus potentially serve as a significant component of a 'universal identification system', whether desirable or not.

In line with these plans perhaps, VeriChip acquired Steel Vault Corporation, a credit reporting and identity security service provider, to form a combined company called PositiveID. As VeriChip (now known as PositiveID) noted, in its quarterly 10-Q report, "[b]eginning in the fourth quarter of 2009, with the acquisition of Steel Vault, the Company intends to pursue its strategy to offer identification tools and technologies for consumers and businesses".[601] Perhaps, the acquisition of Steel Vault could also be linked to the possible long-term intention of linking HIMs to financial information or credit card data.

RFID implants could also replace ordinary keys or RFID security clearance badges/contactless cards as the means of opening doors or gaining access to secure areas. Already, for example, there was talk in Texas and in the US Congress on whether or not

600 Grossman, Lev. "Meet the Chipsons" (Time Magazine, 11 March 2002), available at: http://www.time.com/time/magazine/article/0,9171,1001972-2,00.html

601 Positive ID Corporation, Form 10-Q for the quarterly period ended September 30, 2009.

airport employees should be mandated to have a microchip implanted.[602] Employees themselves could essentially become their entrance or security pass. Since RFID is already used immensely in the form of contactless cards for physical access control at places of business, replacing RFID cards with RFID implants will not require a great deal of further investment. However, in addition to keeping track of employees' comings and goings for time registration, HIMs (like RFID-embedded access cards) could also keep track of their movements within the workplace or office space and not just when entering or exiting the building.

There have been escalating calls for HIMs to be implanted into convicted pedophiles/sex offenders, violent criminals and even into HIV carriers. For example, in Oklahoma legislators debated whether to authorize HIMs in prisoners convicted of violent crimes.[603] With the overcrowding of prisons in the US, particularly in California, and a nationwide prison population now at over two million and growing, GPS implants could be used to relieve overcrowded prisons and rising costs by freeing people accused of non-violent crimes or could even be used as an alternative to prison for certain non-violent crimes. In the US, like in the UK, electronic monitoring in the form of GPS bracelets has been commonly introduced as a condition of being granted bail, an early release or parole. There are already tens of thousands of electronically tracked offenders in the US.[604] GPS bracelets are essentially just one step behind GPS implants and, according to Steve Aninye, President of Omnilink Systems, "the [US] justice system is interested in an implantable [GPS] device".[605] RFID implants could also be implanted into prisoners convicted of violent crimes and still in prison, which is equally just one step ahead of the RFID bracelets, developed by Alanco Technologies, being worn by thousands of inmates within several prisons across the US.

HIMs could be implanted in immigrants when they enter the US and used to track their movements and to locate them once their work visa has expired. Scott R. Silverman, the Chief Executive Officer of VeriChip, and largest shareholder, similarly proposed implanting HIMs in immigrants and guest workers during an interview on

---

602 see a *KENS 5* Eyewitness News broadcast video on 14 May 2007 available on YouTube, at: http://www.youtube.com/watch?v=Keo2TR1Zouw

603 Talley, Tim. "House rejects microchip implants for violent criminals" (Associated Press, 25 May 2007), available at: http://www.examiner-enterprise.com/articles/2007/05/24/news/state/news440.txt

604 see Hunt, V. Daniel., Albert Puglia, and Mike Puglia. *RFID-A Guideline to Radio Frequency Identification* (Wiley, 2007), p. 81.

605 Cozzens, Tracy. "Implant Issues More than Skin Deep" (GPS World, 1 June 2006), available at: http://uc.gpsworld.com/gpsuc/article/articleDetail.jsp?id=364980

"Fox & Friends", a program on FoxNews, adding that "We [VeriChip] have talked to many people in Washington about using it...."[606] HIMs could also be used to track border crossings of US citizens. Already, RFID smart cards have been tested at the US-Mexico border and Washington State and the DHS are testing licenses with embedded RFID microchips.

RFID implants could be implanted in soldiers as a means of identifying their corpses, while GPS implants could monitor individual troop movements in a battlefield. GPS, after all, was apparently developed in the first place to monitor the movements of troops and equipment. VeriChip has already lobbied the Pentagon to replace military dog tags with HIMs,[607] and the RFID bracelets, developed by Precision Dynamics Corporation and Texas Instruments, have been deployed in Iraq to track the location and status of wounded soldiers.[608] In addition, police officers could also be required to have a RFID implant implanted in order to deploy 'smart guns', or a GPS implant in order to instantly determine the closest officer to dispatch to a crime scene.

HIMs could even be implanted in children in order to tackle poor attendance or tardiness and record the entering and exiting on school buses. As a pre-requisite to fully-fledged GPS implants, school buses could instead be fitted with GPS devices to enable parents to know the bus's current location by logging onto a secure website. There have already been calls for mandating that children wear RFID tags or to attach them to their school bags[609] and pilot programs to test the effectiveness of such schemes.[610]

There is even a potentially strong market for HIMs in sports, based on their capability for tracking the performance of athletes. Already, RFID tags were used in the 2007 Boston Marathon.[611]

---

606 "Verichip Injects Itself Into Immigration Debate" (Spy Chips, 18 May 2006), available at: http://www.spychips.com/press-releases/verichip-immigration.html

607 see Francis, David and Myers, Bill. "Company trying to get under soldiers' skin" (The Examiner, 21 August 2006), available at: http://www.examiner.com/a-232630~Company_trying_to_get_under_soldiers__skin.html

608 Precision Dynamics Corp., Press Release, 20 May 2003, available at: http://www.pdcorp.com/en-us/company/pr2003-pdc-rfid-navy-use.html

609 Leff, L. "Students ordered to wear tracking tags" (Associated Press, 9 February 2005), available at: http://www.msnbc.msn.com/id/6942751/

610 Gutierrez, David. "U.S. School District to Begin Microchipping Students" (Natural News, 16 June 2008), available at: http://www.naturalnews.com/023445.html

611 see O'Connor, Fred. "RFID helps the Boston Marathon run" (PC World, 9 April 2007), available at: http://www.washingtonpost.com/wp-dyn/content/article/2007/04/09/AR2007040901011.html

The increase in web-based digital or electronic medical/health records or 'health IT', as part of the greater movement towards e-Health, may coincide with the increased implantation of HIMs, particularly if Medicare or private insurance companies cover the costs (Spivey, 2009). During the beginning of 2009, US President Barack Obama announced his plan to computerize the entire country's health records within five years.[612] Companies with a vested interest in the technology, such as Philips, and lobbying organizations, such as the Center for Health Transformation, are promoting RFID technology as the main component of electronic health records (EHR). RFID technology has already been significantly deployed within the healthcare sector in the US (Cannataci, 2011).

This would be consistent with the strong potential for RFID implants to become a carrier of the Unique Health Identifier (UHID), as Spivey (2009) asserts.[613] The UHID is a number composed of 28 numeric digits, which will eventually serve to facilitate the nationwide electronic availability of personally identifiable health/medical information.[614]

The American Recovery and Reinvestment Act of 2009 allocated the billions of dollars needed to bring about the widespread digitization of medical records.[615] The bill also extensively provides the necessary provisions for EHRs and sets a goal for the creation and utilization of an EHR for each US citizen by 2014,[616] i.e. within five years, as President Obama earlier announced. Of course, (web-based) EHRs present additional data security and serious privacy concerns for personal health data that this dissertation will not go into.

RFID implants and associated web-based databases, such as those of VeriChip, fit in perfectly with the American Recovery and Reinvestment Act's definition of "health information technology" as the "hardware, software, integrated technologies or related

[612] see Goldman, David. "Obama's big idea: Digital health records" (CNN, 12 January, 2009), available at: http://money.cnn.com/2009/01/12/technology/stimulus_health_care/index.htm

[613] see Spivey, Crystal. *Breathing New Life Into HIPAA's UHID – Is The FDA's Green Light To The VeriChip™ The Prince Charming Sleeping Beauty Has Been Waiting For?* (9 DePaul Journal of Health Care Law, 2005-06), pp. 1317-1342.

[614] Health Insurance Portability and Accountability Act of 1996, Public Law 104-191.
However, as widely recognized among privacy law experts, the problem is that the Health Insurance Portability and Accountability Act 1996 (HIPAA), the federal medical privacy bill, does not cover web-based medical records.

[615] Incorporating new and unrelated legislation into spending bills is not unheard of. For example, the Real ID Act 2005 was astonishingly attached to a spending bill. See Division B of H.R.1268, An act making Emergency Supplemental Appropriations for Defense, the Global War on Terror, and Tsunami Relief, for the fiscal year ending September 30, 2005.

[616] American Recovery and Reinvestment Act of 2009, Sec. 3001, (3)(A)(ii).

licenses, intellectual property, upgrades, or packaged solutions sold as services that are designed for or support the use by healthcare entities or patients for the electronic creation, maintenance, access, or exchange of health information".[617]

Already, manufacturers of implantable medical devices sold in the US are required by the Food and Drug Administration Amendments Act of 2007 to ensure that implantable medical devices are identifiable and trackable via a 'unique device identifier' (UDI). RFID technology is increasingly being used to electronically track medical devices. An implantable medical device with an embedded RFID microchip could potentially have similar identification and tracking capabilities to RFID implants.

Perhaps, the next step would be for the US Government to request health insurance providers to cover the costs of the RFID implant procedure. Medicare could also eventually cover the costs. In 2008, the American Medical Directors Association (AMDA) initiated a clinical study to evaluate whether VeriChip's VeriMed Patient Identification System can improve patient outcomes. The study is meant to involve up to 10 facilities and 100 participants. Upon completion of the study, VeriChip intends to use the results to seek reimbursement approval from insurance companies and the Centers for Medicare & Medicaid Services.[618]

A hospital in New Jersey (US) and the major health insurance provider Horizon Blue Cross Blue Shield began recruiting volunteers in 2006 to have a RFID implant implanted in a two-year trial to determine if the implants reduce healthcare costs.[619] Already, US President Obama has advocated that EHRs could create jobs and reduce healthcare costs in the long-term. As a result, there is perhaps a possibility that RFID implants could become more common, if they are viewed as a means of reducing healthcare costs in conjunction with EHRs.

Moreover, VeriChip, the exclusive provider of RFID implants authorized for human implantation, announced that it has obtained exclusive licenses for two additional patents, which will help the company to develop implantable virus detection systems in humans. The patents, held by VeriChip partner Receptors LLC, relate to biosensors that can detect the H1N1 virus and other viruses, and biological threats. The technology will reportedly combine with VeriChip's RFID implant technology to develop a 'triage detection system'.

---

617 *Ibid.*, Sec. 3000 (5).

618 see VeriChip Corp., Press Release, available at: http://www.reuters.com/article/pressRelease/idUS137195+08-Jan-2008+BW20080108

619 see M.L. Baker. "Insurers Study Implanting RFID Chips in Patients", *eWeek.com*, 19 July 2006, available at: http://www.eweek.com/c/a/Health-Care-IT/Insurers-Study-Implanting-RFID-Chips-in-Patients/

While the ongoing economic crisis and existing health legislation is ripe for RFID implants, even global warming (or climate change), can be used as an excuse to track the movements of people and generate a carbon footprint report or 'green report card' for each and every person.[620] This can already be done with GPS-equipped smartphones using the application *Ecorio*, which uses GPS to track every movement and uses the data to generate a personalized carbon footprint report,[621] or via GPS devices in vehicles to levy a road tax by kilometer/mile, which was proposed in the Netherlands. Although this report would be incomplete, governments could one day perhaps use this information to tax each person according to the results of their report or to monitor the use of their personal 'carbon allowance'.[622]

For now, HIMs are implanted voluntarily. Under the National Animal Identification System (NAIS), RFID ear tags or injectable RFID tags are being used to identify and track millions of livestock animals to enable the US Government to respond quickly to disease. The animals are each identified by a 15-digit Animal Identification Number (AIN). Some critics of the plan have already voiced their concerns that animals could be the forerunner of a similar system for humans.[623] There is, however, no evidence that there are plans for HIMs to be mandated for individuals.

On the other hand, as Ramesh (1997) argues, "[a] national identification system via microchip implants could be achieved in two stages. Upon introduction as a voluntary system, the microchip implantation will appear to be palatable. After there is a familiarity with the procedure and knowledge of its benefits, implantation would be mandatory".[624] Indeed, history has demonstrated that something voluntary today can become mandatory tomorrow, or at least indirectly mandatory, since its possession could later become necessary to carry out ordinary daily activities. This is already the case today with ID cards in the US, and the same may potentially also prove true for

---

620 see Ecorio, available at: http://www.ecorio.org

621 This concept is gaining traction. During the post-i2010 Public Hearing on "Priorities for a new strategy for European Information Society" held 23 September 2009 in Brussels, a representative from the mobile phone carrier Orange expressed interest in the potential of mobile phones to be used to collect data.

622 The idea for personal 'carbon allowances' for individuals was proposed by the Chairman of the UK's Environment Agency, Lord Smith.

623 see Gumpert, David E. "Animal Tags for People?" (Business Week, 11 January 2007), available at: http://www.businessweek.com/smallbiz/content/jan2007/sb20070111_186325.htm?chan=smallbiz_smallbiz+index+page_today's+top+stories

624 Ramesh, Elaine M. Time Enough? Consequences of Human Microchip Implantation, Franklin Pierce Law Center (1997), available at: http://www.fplc.edu/risk/vol8/fall/ramesh.htm.

HIMs. Moreover, once the coerced implantation of HIMs in parolees and in convicted pedophiles or other convicted criminals is put into effect and the public accepts the potential security benefits, other coerced implantations could similarly materialize.

However, HIMs do not necessarily have to be something that governments enforce upon us. Mandatory implantation may not be required as consumers begin to want HIMs anyhow or are enticed to want one on the basis of security, personal safety, consumer and medical benefits. The ongoing proliferation of tracking technologies and of LBS on smartphones implies that consumers already accept location-aware applications and the amenities that location-awareness provides. If many people are already willingly, some quite enthusiastically, to broadcast their location, it is likely that these people will begin to accept or even desire RFID or GPS implants, particularly as digital inclusion (or e-Inclusion) increasingly becomes a means of social inclusion, or as digital exclusion (e-Exclusion) more and more translates into social exclusion.

HIMs could even become a status symbol or made to look fashionable, with the increasing array of hypothetical scenarios depicted in popular culture to familiarize society with HIMs and to condition or program people's acceptance through mainstream media and commercials.[625] As Aarts and de Ruyter (2009) question "how long will it be before we accept the implantation of chips for non-medical reasons?" Further adding, "[a]ttitudes to the body are already changing. Body piercing, tattoos and cosmetic surgery are much more common than a generation ago" (2009, p. 12).

Still, fear, above all else, and not the lure of fashion or the satisfaction of a desire, nor the struggle for efficiency or progress, will likely be the main catalyst for HIMs. Just like other tragic disasters and crises have led to negative effects on freedom and privacy, the threat of terrorism, the ever-increasing crime rate and apparently worsening global environmental crisis could lead to further tracking of people's movements.

---

625 There are numerous examples in mainstream media. The relevant clips that depict HIMs can be found on YouTube. In the film, *Casino Royal* (2006), the British spy James Bond 007, and in the film, *Demolition Man*, the character John Spartan are both implanted with a microchip in order to track their movements. In the television series *Heroes* (Series 3, Episode 14), one of the characters is even implanted with a "GPS implant". In the BBC drama *The Last Enemy* (2008), a plot to implant everyone with a RFID tag is revealed. RFID implants are remarkably described as an "ID that can't be lost, forged or stolen…Its content and function can be adapted to suit my needs. It can be my credit card. It can be door key, my car keys. I'll never lose them again. Eventually it will become universal. Starting at school age, a tag for life". In *CSI Miami* (episode 305), a murdered teenager's VeriChip is removed and scanned to reveal her associated information on a computer screen, which later helps in the investigation. In *Mission: Impossible 2* (2000) a transponder chip is implanted into a main character. More recently, in the film *Hunger Games*, children are implanted with microchips to track their movements. In an IBM televised commercial several years ago on e-Business of the future, a supermarket shopper is shown stuffing RFID-tagged items under his coat and then automatically paying for the items by simply walking through a RFID gateway and without using a credit/debit card or mobile phone, which likely implies he had a RFID implant.

Fear of global warming, fear of a terrorist attack, fear of being kidnapped or murdered and the fear of one's child either being kidnapped or sexually offended are just a few examples. HIMs could slowly just become as ordinary as having an ID number or an RFID-embedded ID card or wearing clothing or carrying items with embedded RFID tags or carrying around GPS-equipped smartphones – all of which exist today.

Nonetheless, any widespread deployment and realization of the diverse practical applications of RFID will require not just interoperability and the necessary infrastructure, but also additional available space in the radio spectrum for the transmission of data over longer distances. This could be accommodated for through the complete switchover from analog to digital TV, which is occurring in the US and gradually in the EU.

7.6.3 Actual and potential international deployment

Kevin Haggerty also foresees that the escalation of HIMs will start in countries at the periphery of the Western world.[626] Remarkably, his prediction is already gaining traction.

In the Indonesian province of Papua, it was reported that carriers of HIV are to be implanted with microchips under a bill backed by the provincial parliament to track and punish anyone who deliberately infects others.[627] In Mexico, the country's Attorney General (former), Rafael Macedo, and members of his staff were reportedly implanted with RFID implants as a means of controlling access to a sensitive records room. Other people in Mexico are getting HIMs implanted, like the one developed by Xega, to counter the threat of being kidnapped. In addition, the Congressional Record shows that Colombian President Álvaro Uribe told (former) US Senator Arlen Specter (D-Pa) "he would consider having Colombian workers have microchips implanted into their bodies before they are permitted to enter the United States to work on a seasonal basis".[628]

HIMs are also slowly spreading beyond America's borders into the Western world. In Barcelona, Spain and in Rotterdam, the Netherlands, the Baja Beach nightclubs infamously began to implant HIMs in those wanting to jump entrance lines, open doors to VIP lounges and pay for drinks without cash or debit/credit cards. However, much of this is just a publicity stunt of the nightclub's owner. The parents of Danielle Duval,

---

626 Haggerty, Kevin. "One generation is all they need" (The Star, 10 December 2006) available at: http://www.thestar.com/sciencetech/article/136744

627 see "Indonesian AIDS patients face microchip monitoring" (Associated Press, 24 November 2008), available at: http://www.guardian.co.uk/world/2008/nov/24/indonesia-aids

628 Trip to Colombia, Peru, Brazil and Dominican Republic, U.S. Senate, 25 April 2006, p. S3495.

an 11 year-old girl, reportedly took the extraordinary step of having their daughter implanted with a transponder microchip so that her movements could be traced if she were to be abducted. They decided to do so after the abduction and murder of the schoolgirls Holly Wells and Jessica Chapman.[629] The issue came up again in the wake of the disappearance of the British child Madeleine McCann in Portugal. The Times published an article asking whether children should be implanted.[630] Even more controversial, a leaked British policy review document revealed that the British Government even considered implanting RFID implants in the mentally ill.[631]

7.7 ALTERNATIVES TO HIMs

There are indeed alternative systems and/or devices to RFID and GPS implants on the market or in development that can fulfill, to a certain degree, the same goals.

Direct competition for VeriChip's human-implantable RFID tags for medical purposes include the non-RFID, low-tech alternative of MedicAlert's jewelry bracelets that are engraved with the wearer's primary medical conditions and an ID number. However, MedicAlert's bracelet is not linked to hospital databases and can easily be removed. Another potential alternative is "medical tattoos", which can include basic information on a person's chronic diseases or allergies. Other non-RFID alternatives for medical purposes include: smart chip cards, which can be used to both access the medical history of patients at hospitals and store medical history; the CARE Memory Band, which can be connected to a computer by medical personnel to access medical data stored on the wrist bracelet; and simple bar-code wristbands. However, since RFID is a type of 'over-the-air' technology it does not require direct line-of-sight and can be read through non-metallic materials, unlike bar codes. RFID microchips also have a larger memory storage capacity than bar codes. The advantages of RFID tags have led to the belief that they will eventually replace bar codes in general, but this has yet to happen.

SmartWear Technologies produces wearable RFID devices that can equally be used to provide medical information to paramedics. Other RFID alternatives for medical

629 Wilson, Jamie. "Girl to get tracker implant to ease parents' fears" (The Guardian, 3 September), available at: http://www.guardian.co.uk/uk/2002/sep/03/schools.childprotection2

630 Midgley, Carol. "Would an implanted chip help to keep my child safe?" (Times Online, 15 May 2007), available at: http://women.timesonline.co.uk/tol/life_and_style/women/families/article1788169.ece

631 Jones, George. "Microchips for mentally ill planned in shake-up" (The Telegraph, 18 January 2007), available at: http://www.telegraph.co.uk/news/uknews/1539716/Microchips-for-mentally-ill-planned-in-shake-up.html

purposes include Precision Dynamics Corp.'s Smart Band RFID wristbands and GenTag's RFID wireless skin patches, which can be used to identify patients and capture and verify data before delivering medication or conducting surgery. However, both the Smart Band and GenTag's RFID wireless skin patches are designed for use after being admitted within hospitals and are disposable. The Smart Band is also marketed for use as a means of cashless purchases, keyless hotel entry and access control, while GenTag also markets its RFID wireless skin patches for use in entrance control, child ID and location tracking at amusement parks and for cashless payment transactions at hotels and casinos. Ident Technologies has developed a system named Skinplex®, which is composed of small signal generators worn closely on the body that transmit coded data to one or more receivers to identify and/or track the person concerned.

The TSI PRISM system, developed by Alanco Technologies, Inc. for use in correctional facilities, uses a RFID-enabled wrist bracelet to monitor the location of prison inmates in real-time.[632] To track children's movements while in the park, Legoland in Denmark uses a combination of RFID tags in bracelets and Wi-Fi.[633]

Once again, instead of implanting RFID microchips into the human body for identification purposes, the microchips can instead be embedded in ID cards or state driver's licenses, a method, which is currently being piloted in the US.

Alternatives to GPS implants, include GPS bracelets developed by Pro Tech or the GPS bracelets developed by Omnilink Systems that are combined with cellular technology. GPS bracelets are already being attached to parolees and sex offenders to create "mobile exclusion zones".[634] RemoteMDx Inc. delivers a similar monitoring system to keep track of offenders no matter where they may be. Also on the market include Fujitsu's Tag Locator V2, which uses GPS to detect its location and RFID to send that data along with its unique ID number to a reader, and Lego-James, a multi-faceted bracelet that allows parents to track the location of their children through 3G technology and the use of a GPS receiver. BlackBox GPS' personal locators, which resemble a pager, allows users to know where the wearer is located at all times anywhere in the world.[635] TRACKiT is a similar GPS device and service that locates the object or person

---

632 TSI Prism, at http://www.tsiprism.com; see Sofge, Erik. "High-Tech Lockup: Inside 4 Next-Gen Prison Security Systems" (PopularMechanics, 12 February 2008), available at: http://www.popularmechanics.com/technology/military_law/4248844.html?page=2

633 Collins, Jonathan. "Lost and Found in Legoland" (RFID Journal, 28 April 2004), available at: http://www.rfidjournal.com/article/view/921/1/1

634 Omnilink, at http://www.omnilinksystems.com/solutions_domestic_violence_monitoring.php

635 BlackBox GPS, available at: http://www.blackboxgps.com/cms/

the device is attached to and enables the user(s) to view the location on the Internet and receive sends text messages or emails if the tracked object or person ventures outside an invisible, customizable perimeter, also known as a ‘geo-fence’. XACT|TRAX and the Little Buddy Child Tracker are other similar devices. Lok8u produces Num8, an inexpensive device, which resembles a wristwatch, that can be used by parents to locate and track their children at all times via the Internet and via text messages on a cell phone. GTX Corp. has developed a “GPS smart shoe”, which has an embedded GPS chip and enables the wearer to view their location data in real-time on a Google map via a smartphone or PDA. Other less popular or less likely alternatives to GPS implants include wearable computers such as Eurotech’s Zypad WL 1000, which is a wrist-worn touch screen computer with GPS and Wi-Fi connectivity.

Alternatives for implantable military dog tags include the Defense Advanced Research Projects Agency’s (DARPA) personal radio beacons, which are worn on the soldier’s uniform and can provide location data without the use of GPS, and Thales’ MILTRAK, which is a device similar to a cell phone and also capable of transmitting and receiving location data.

However, none of these alternatives entirely possess the benefits and attributes of a HIM. The fact that HIMs essentially cannot be easily lost, removed or tampered with is what might make them more appealing to parents, corporations, the medical industry and governments. HIMs are everlasting, convenient and cannot be forgotten. For consumers, HIMs could be appealing because they are not uncomfortable to wear.

7.8 LAWS, CODES, DECISIONS AND OTHER LEGAL/POLICY INSTRUMENTS OF SPECIAL RELEVANCE IN THE US

7.8.1 Constitutionally protected rights

The Fourth Amendment of the US Constitution, which protects individuals from “unreasonable searches and seizures”, conducted by the US Government and serves as the basis of the right to privacy in the US, reads:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

The Fourth Amendment is invoked when the US Government infringes upon a person's 'reasonable expectation' of privacy.

Also relevant is the Fifth Amendment, which states that no individual "shall be compelled in any criminal case to be a witness against himself". In other words, individuals cannot forcibly incriminate themselves. However, only written or spoken words are considered self-incriminating and covered by the Fifth Amendment, while elements, such as blood samples or DNA samples, are not. In Schmerber v. California, for example, a case concerning whether or not blood forcibly withdrawn from Armando Schmerber while in hospital recovering from a traffic accident could be used to prove intoxication, the US Supreme Court affirmed, "blood test evidence, although an incriminating product of compulsion, was neither petitioner's testimony nor evidence relating to some communicative act or writing by the petitioner, it was not inadmissible on privilege grounds".[636]

7.8.2 Federal statutory laws

Telecommunication companies have the capacity to collect vast amounts of information on their customers when they use a telecommunication service. The Telecommunications Act of 1996 (hereinafter called the "Telecom Act") terms this information Customer Proprietary Network Information (CPNI) and regulates when and how telecom companies may use and disclose CPNI to third parties.[637]

The Federal Communications Commission (FCC) adopted formal rules, later codified in Federal regulations, requiring cell phones to be location-capable and wireless service providers to develop the capability for providing precise location information of wireless emergency callers, known as Enhanced 911 (E911) capabilities.[638]

Accordingly, the definition of CPNI[639] was amended by the Wireless Communications and Public Safety Act of 1999[640] to include "location" and subsection (f) was added to Section 222 of Title 47 U.S.C. Chapter 5, Subchapter II, Part I, explicitly

---

[636] *Schmerber v. California*, 384 U.S. 757, 765 (1966).

[637] see Title 47 U.S.C. Chapter 5, Subchapter II, Part I, § 222.

[638] see Title 47 C.F.R. Ch. I, § 20.18.

[639] see Title 47 U.S.C. Chapter 5, Subchapter II, Part I, § 222 (h)(1)(A).

[640] Public Law 106-81, 113 Stat. 1286 (1999).

mandating, with certain exceptions, that "express prior authorization of the customer" is required to disclose, use or access call location information.[641]

The growing use of mobile phones, or other wireless/digital communication technologies, also brought about the need for new legislation to ensure that the use of pen registers and trap and trace devices by law enforcement agencies is still effective, in order to preserve their ability to intercept communications and obtain "call-identifying information". The Communications Assistance for Law Enforcement Act of 1994 (CALEA)[642] provides that telecommunications carriers and manufacturers of telecommunications equipment ensure their equipment, facilities, and services are capable of being used by law enforcement for surveillance purposes.[643] However, as CALEA specifies, "call-identifying information shall not include any information that may disclose the physical location of the subscriber" when "acquired solely pursuant to the authority for pen registers and trap and trace devices".[644]

The Electronic Communications Privacy Act 1986 (ECPA) regulates government access to private/stored electronic communications.[645] Government entities require a court order for access, which may be issued if the government entity "offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation".[646]

With regards to the laws specifically relevant to RFID implants, the US Congress is paving the way forward for a national ID card embedded with an RFID microchip. The REAL ID Act of 2005 mandates that all state driver's licenses and ID cards conform to certain standards.[647] While ID cards are voluntary in the US, they are nonetheless required for a wide variety of everyday purposes. Although the REAL ID Act does not specifically require that driver's licenses contain RFID, the REAL ID Act mandates that

---

641 Exceptions to this rule include, for example, when there is a need to provide the location information of the caller to a public safety answering point, emergency medical service provider, public safety, fire service, or law enforcement official, etc., in order to respond to the caller's emergency. see Title 47 U.S.C. Chapter 5, Subchapter II, Part I, § 222(d)(4)(A).

642 Public Law No. 103-414, 108 Stat. 4279.

643 Title 47 U.S.C. Chapter 9, Subchapter I, § 1002 (a).

644 *Ibid.*, § 1002 (2) (B).

645 Public Law No. 99-508, 100 Stat. 1848 (1986).

646 Title 18 U.S.C Part I, Chapter 121 § 2703(d).

647 see Real ID Act of 2005, Public Law No. 109-13, § 201-207.

all state driver's licenses and ID cards include machine-readable technology, among other requirements, and gives the Secretary of Homeland Security the authority to do so.[648] RFID is a type of machine-readable technology and, as already mentioned, RFID microchips are indeed being embedded in state driver's licenses and in US passports.[649] However, few US states have implemented the REAL ID Act and even a number of US states have passed legislation rejecting the REAL ID Act. Since then, S. 1261, titled "Providing for Additional Security in States' Identification Act of 2009" or the "Pass ID Act", which is similar to the REAL ID Act, was proposed in the US Senate, possibly to replace the failed attempt by the REAL ID Act.

The Identity Theft and Assumption Deterrence Act of 1998 criminalizes the intentional transfer, possession or use, without lawful authority, a "means of identification" of another person. A means of identification may include, in addition to any name, social security number, etc., a unique electronic identification number.[650] Therefore, regardless whether or not a RFID implant is linked to personally identifiable information, the unique ID number of a RFID implant alone should qualify as personal identifiable information under US statutory law, since it legally constitutes a means of identification.

The printout of location information, generated by both GPS and RFID implants, could be considered originals and thus admissible as evidence in a court of law. As the Federal Rules of Legal Evidence confirms:

> An "original" of a photograph includes the negative or any print therefrom. If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an "original".[651]

Once again, however, wrongfully obtained evidence, in violation of the Fourth Amendment, may be excluded from criminal proceedings in a court of law,[652] known as the "exclusionary rule". As Rule 402 states:

> All relevant evidence is admissible, except as otherwise provided by the Constitution of the United States, by Act of Congress, by these rules, or by other

---

648 *Ibid*. § 205(a).

649 RFID tags are also being embedded in passports around the world, notably in EU Member States, to comply with US demands and international standards.

650 see Public Law No. 105-318, 112 Stat. 3007, codified at Title 18, U.S.C. Part I, Chapter 47, § 1028 (d)(7).

651 Federal Rules of Legal Evidence, Article X, Rule 1001(3).

652 see *Weeks v. United States,* 232 U.S. 383 (1914); Mapp v. Ohio, 367 U.S. 643, 655 (1961).

rules prescribed by the Supreme Court pursuant to statutory authority. Evidence which is not relevant is not admissible.

7.8.3 Tort law

Tort law is relevant for the private use of the location information generated by HIMs. There are four invasion of privacy torts, of which one or more are recognized by courts in practically all states in the US, albeit to some extent and sometimes tentatively (McClurg, 1995). The Restatement (Second) of Torts reads:

> (1) One who invades the right of privacy of another is subject to liability for the resulting harm to the interests of the other.
> (2) The right of privacy is invaded by:
> (a) unreasonable intrusion upon the seclusion of another, as stated in 652B; or
> (b) appropriation of the other's name or likeness, as stated in 652C; or
> (c) unreasonable publicity given to the other's private life, as stated in 652D; or
> (d) publicity that unreasonably places the other in a false light before the public, as stated in 652E.[653]

The most potentially relevant of the four torts for the unauthorized collection and disclosure of location information is the tort of "unreasonable intrusion upon the seclusion of another" (McClurg, 1995), which is defined as:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.[654]

7.8.4 Case law

There is judicial precedent in the US regarding the use of tracking (or location-detecting) devices by law enforcement agencies, which is relevant to the tracking capabilities of both GPS and RFID implants.

---

653 Restatement (Second) of Torts, § 652A (1977).

654 *Ibid.*, § 652B.

In *United States v. Knotts*, law enforcement agents placed a RF tracking device on a chloroform bottle that one of the defendants purchased and then followed him to what was later suspected to be a drug laboratory. The US Supreme Court held that the driver in his automobile had "no reasonable expectation of privacy in his movements from one place to another" while in public.[655] The US Supreme Court also held:

> The fact that the officers in this case relied not only on visual surveillance, but also on the use of the beeper to signal the presence of [Darryl] Petschen's automobile to the police receiver, does not alter the situation. Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case.[656]

Around a year later, in *United States v. Karo*, the US Supreme Court held that no showing of evidence or probable cause is required to observe information conveyed in areas observable to the public.[657] Similarly, in *Oliver v. United States,* the US Supreme Court also held that there is no reasonable expectation of privacy in 'open fields'.[658] Nevertheless, while *United States v. Karo* reaffirmed that an individual has no reasonable expectation of privacy of his movements in public, the US Supreme Court recognized that Fourth Amendment protections are applicable when the RF device moves out of a public place and into a private space.[659]

Moreover, in *Katz v. United States*, the US Supreme Court earlier on held that whatever a person "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected"[660] (emphasis added), as long as the person concerned exhibits first "an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as reasonable".[661] This is commonly known as the *Katz* test.

---

655 *United States v. Knotts*, 460 U.S. 276, 281 (1983).

656 *Ibid.*, at 282.

657 see *United States v. Karo*, 468 U.S. 705 (1984).

658 see *Oliver v. United States*, 466 U.S. 170 (1984).

659 see 468 U.S., at 714.

660 *Katz v. United States*, 389 U.S. 347, 351 (1967).

661 *Ibid.*, at 361. Concurring opinion of Justice Harlan.

In *Kyllo v. United States*, the US Supreme Court infuses into the interpretation of the Fourth Amendment the notion that law enforcement does not engage in a search under the Fourth Amendment when it uses a technology or device that is in general public use.[662] However, more recently, in *United States v. Jones,* the US Supreme Court ruled that the installation and use of a GPS tracking device to monitor vehicle movements constitutes a search under the Fourth Amendment.

With regards to the legality of forced implantation, case law in the US has long recognized that individuals have the right to physically or bodily integrity and the protection from bodily intrusions. As Justice Cardozo asserts, "[e]very human being of adult years and sound mind has a right to determine what shall be done with his own body".[663] There are certain exceptions in light of the needs of society. For example, mandatory random drug tests for certain lines of work have been upheld. In *Skinner v. Railway Labor Executives Association*, the US Supreme Court ruled that drug and alcohol testing of railroad employees, engaged in tasks that pose a threat to public safety if errors are to occur, was justified,[664] and, in *National Treasury Employees Union v. Von Raab*, the US Supreme Court held that random drug testing of employees who carry firearms is equally justified.[665]

With regards to the right to refuse to be identified, in *Hiibel v. Sixth Judicial District Court of Nevada, Humboldt County*, the US Supreme Court upheld that individuals are not permitted to refuse to identify themselves to a law enforcement officer during the conduct of an investigation.[666]

---

662 *Kyllo v. United States*, 533 U.S. 27, 34 (2001).

663 *Schloendorff v. Society of the N.Y. Hosp*., 211 N.Y. 125, 129 (1914).

664 *Skinner v. Railway Labor Executives Association*, 489 U.S. 602 (1989)

665 *National Treasury Employees Union v. Von Raab*, 489 U.S. 656 (1989)

666 *Hiibel v. Sixth Judicial District Court of Nevada, Humboldt County*, 542 U.S. 177 (2004).

7.8.5 State statutory laws

Although there are no federal statutory laws pertaining to HIMs, there are a number of relevant state legislative acts that have been signed into law. For example, North Dakota Senate Bill 2415 (2007) prohibits anyone from requiring another person to have a HIM implanted. Wisconsin has a similar law, which requires that "[n]o person may require an individual to undergo the implanting of a microchip".[667] California Senate Bill 362 provides that no person may "require, coerce, or compel any other individual to undergo the subcutaneous implanting of an identification device".[668] Washington criminalized the unauthorized reading of an RFID identification device "for the purpose of fraud, identity theft, or for any other illegal purpose" as a class C felony".[669] In Pennsylvania, H.B. 2374 prohibits anyone from requiring another person to undergo the subcutaneous implanting of an identification device. The bill passed Pennsylvania's House of Representatives. Other state legislatures have also passed legislation prohibiting the involuntary implantation of HIMs. It is important, however, to point out here that these state laws have not banned HIMs, but have rather prohibited their forced implantation. A number of other states have introduced legislation relating to the use of RFID, but most address the use of RFID tags/microchips embedded in retail products.

Some legislative proposals pertaining to the use of RFID for tracking purposes have also failed to become law. In Rhode Island, H.B. 5929, which attempted to prohibit the state's Government from tracking the movement or identity of an employee, student or client as a condition of obtaining a benefit or services, actually made it to the state governor's desk, but was strangely vetoed. The Identity Information Protection Act of 2005, among other security and privacy guarantees, attempted to make it a crime in California to "skim" (i.e. to scan in an unauthorized manner) an individual's RFID-enabled identification document in order to obtain personal data without the knowledge of that individual.[670] However, this balanced and thoughtful bill was vetoed.[671]

---

[667] see Wisconsin Statute 146.25.

[668] see California Civil Code, Section 52.7 (a).

[669] see Title 19, Chapter 19.300, § 19.300.020.

[670] California Senate Bill 768.

[671] The (former) Governor of California, Arnold Schwarzenegger, explained that he vetoed the legislation because it "may inhibit various state agencies from procuring technology that could enhance and streamline operations, reduce expenses and improve customer service to the public and may unnecessarily restrict state agencies" and "may unduly burden the numerous beneficial new applications of contactless technology". see A Letter from the Governor of California to Members of the California State Senate, available at: http://gov.ca.gov/pdf/press/sb_768_veto.pdf

A second attempt[672] was also vetoed, but finally California Senate Bill 31 (2007) was signed into law, which makes skimming of RFID-enabled identification documents a crime punishable with imprisonment. In Maryland, H.B. 1401, which aimed to prohibit an employer from requiring or compelling an employee to undergo the subcutaneous implantation of a RFID tag, was not even put to a vote.

Existing laws, which address stalking and cyberstalking or electronic stalking, could be relevant to the tracking capabilities of HIMs. All 50 states, the District of Columbia and the US Government have enacted various laws making the act of stalking a felony (Miller, 2001, p. 36). Federal law is applicable in inter-state stalking.[673] Cyberstalking or electronic stalking is essentially the use of the Internet or a telecommunications or electronic communications device to threaten, harass or annoy another person. Federal law prohibits inter-state or foreign electronic stalking[674] and a number of states have also prohibited electronic stalking.

Moreover, nearly all states have similar laws requiring convicted sex offenders and/or certain individuals convicted of a felony to wear a GPS tracking device (GPS bracelet), in order for police to track their movements. Important differences, however, are whether or not the decision to do so is based on individual based assessments (Hinson, 2008). For example, Massachusetts Senate Bill No. 1351 provides for an individualized 'dangerousness assessment', while Florida's Jessica Lunford Act does not, as pointed out by Hinson (2008).[675] There is, however, at present, no equivalent federal law on the electronic monitoring of convicted sex offenders.

7.8.6 Administrative decisions

In 2004, the FDA approved the use of RFID implants as a Class II medical device.[676] This serves as the single most important official administrative decision regarding RFID implants (i.e. HIMs).

---

672 California Senate Bill 30 (Identity Information Protection Act of 2007).

673 Title *18 U.S.C. Part I, Chapter 110A, § 2261A;* see Miller, Neal. *Stalking Laws and Implementation Practices: A National Review for Policymakers and Practitioners* (2001), p. 36, available at: http://www.ncjrs.gov/pdffiles1/nij/grants/197066.pdf

674 Title 47 U.S.C. Chapter 5, Subchapter II, Part I, § 223.

675 see Hinson, Zoila. *GPS monitoring and constitutional rights* (43 Harvard Civil Rights-Civil Liberties Law Review, 2008), pp. 285-288.

676 Federal Register, Volume 69, Number 237, 10 December 2004, pp. 71702-71704.

7.8.7 Standards, guidelines and self-regulations (soft laws)

The privacy policy of VeriChip Corp. was first declared in a 'Six Point Privacy Statement', which read as follows:

1. VeriChip should be voluntary and voluntary only. No person, no employer, no government should force anyone to get "chipped."
2. Privacy must be a priority at the highest levels of our organization and as such we will have a Chief Privacy Officer who, with privacy experts, will be charged with addressing the day-to-day global evolution of this technology.
3. We will immediately address privacy and patients' rights in all consumer, distributor and medical documents related to VeriChip
4. VeriChip subscribers are able have their chip removed and discontinued at any time.
5. Privacy means different things to different people, so only the VeriChip customer should designate the groups that may have access to his or her data base information.
6. We pledge to thoughtfully, openly and considerately engage government, privacy groups, the industry and consumers to assure that the adoption of VeriChip and RFID technology is through education and unity rather than isolation and division.

Since then, VeriChip's full privacy policy has changed, and is no longer available on the company's new website after changing its name to PositiveID.

The Federal Trade Commission Act (FTC Act) prohibits unfair, deceptive or misrepresented corporate practices. Unfair practices include, for instance, a failure to implement a minimal level of security of personal information, while deceptive practices include a company's failure to actually implement its own registered privacy policies/codes of conduct. The FTC has the authority to enforce the promises companies make as a result of their privacy policies/codes of conduct regarding how they collect, use and secure personal information[677] and the FTC has used this authority on numerous occasions to challenge the data processing practices and policies of companies that cause harm to consumers.

Since doctors are meant to administer the implantation of HIMs, the American Medical Association (AMA), the largest professional organization of physicians and

[677] Title 15 U.S.C. § 41-58, as amended, Section 5 of the FTC Act.

patients in the US, established guidelines to protect patients receiving RFID implants,[678] which are a part of the AMA's medical code of ethics. In the report, titled "Radio Frequency ID Devices in Humans", the AMA acknowledges the important ethical, legal and social issues raised by HIMs and advocates for a greater role of doctors regarding the non-medical uses of the technology.[679]

The National Institute of Standards and Technology (NIST) issued its Guidelines for Securing Radio Frequency Identification (RFID) Systems. The NIST elaborates how to address the privacy concerns of RFID in the context of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980). In addition, the OECD Policy Principles on Radio Frequency Identification were also finalized in 2008.

In recognition of the threats to privacy posed by GIS, the Urban and Regional Information Systems Association (URISA) adopted the GIS Code of Ethics, advocating for the protection of individual privacy and the careful handling of new information discovered about individuals through GIS-based manipulations.

The Cellular Telecommunications and Internet Association (CTIA) adopted the Best Practices and Guidelines for Location Based Services, essentially highlighting the necessity of gaining a user's consent before disclosing his/her location information. In addition, the World Wide Web Consortium (W3C) formed a Geolocation Working Group to develop a set of standards for handling users' location information that ensures both interoperability and privacy.

---

678 Report of the Council on Ethical and Judicial Affairs, CEJA Report 5-A-07, available at: http://www.ama-assn.org/ama1/pub/upload/mm/467/ceja5a07.doc

679 *Ibid.*

7.9 DEFICIENCIES AND DILEMMAS OF THE US LEGAL FRAMEWORK

Based on the principles of privacy and the criteria for determining the adequacy of a legal framework, as outlined in Chapter 3, significant legal deficiencies and dilemmas within US statutory laws, tort law and the ‘reasonable’ expectation of privacy standard (as adopted by US courts) become clear. The ineffectiveness of the US legal framework in upholding the right to privacy against the intrusive capabilities of HIMs is, in this dissertation’s analysis, quite substantial.

First and foremost, in light of the US Supreme Court’s decisions in *United States v. Knotts*, *United States v. Karo* and *Oliver v. United States*, implantees may not have a reasonable expectation of privacy of the location information generated by their HIMs as they move about in public. Location information collected by law enforcement agencies via the scanning of RFID implants or monitoring of GPS implants is, at present, not protected under the Fourth Amendment.

The case law also fails to uphold the general legal ***principle of proportionality*** or ensure that the scanning and/or monitoring of HIMs is proportionate to their purported legitimate aim(s). Given that there is essentially no reasonable expectation of privacy in public, as the law stands now, mass public surveillance and the tracking and recording of people’s movements out in public by the US Government, without any justification whatsoever, could be potentially lawful. Nevertheless, unwarranted mass public surveillance should be considered disproportionate, unreasonable and inappropriate in a free and democratic society.

Although the US Supreme Court, in *Katz v. United States*, held that whatever a person “seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected”,[680] if that person does not take extraordinary steps or affirmative measures to protect his or her privacy, as both Paton-Simpson (2000) and Kearns (1998) separately point out, he or she has no reasonable or subjective expectation of privacy.[681] This is essentially consistent with the findings of the 9th Circuit Court of Appeals in *US v. Kyllo*.[682] “Thus the viewpoint is well established that anyone who does not behave as a ‘reasonable paranoid’ has waived any right to privacy” (Paton-Simpson, 2000, p.

680 *Katz v. United States*, 389 U.S. 347 (1967).

681 see Kearns, Thomas B. T*echnology and the Right to Privacy: The Convergence of Surveillance and Information Privacy Concerns* (7 William & Mary Bill of Rights Journal, 1998), pp. 975-1011, at 1005; Paton-Simpson, Elizabeth. *Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places* (50 University of Toronto Law Journal 305, 2000), pp. 305-346, at 306.

682 *US v. Kyllo*. 190 F.3d 1041 (9th Circuit, 1999).

306). This interpretation may especially hold true for those who have decided to have a HIM voluntarily implanted.

The “reasonable expectation” of privacy is additionally problematic, since it is presently defined by the privacy-intrusive capabilities of the latest technologies, their availability and the scope and manner of their deployment and use. For instance, consistent with *Kyllo v. United States,*[683] the mass deployment and widespread public use of RFID and GPS technology and GPS tracking devices, as the technologies become more and more readily available, without the appropriate safeguards in place, would surely diminish our privacy expectation level, both meaningfully and legally. As David Wood, in the *Report on the Surveillance Society,* argues, the reasonable expectation of privacy will surely be depressed if people “get used to” increasingly more surveillance.[684] Likewise, as Dr. Peter Zhou, ADS’ chief scientist at the time, similarly proclaimed, “[b]efore there may have been resistance, but not anymore. People are *getting used* to implants. New century, new trend”[685] (emphasis added). In addition, as Minert (2006) points out, the problem is that the reasonable expectation could become just an echo of the government’s expectation of privacy (2006, pp. 1653-54). Moreover, the relatively widespread voluntary implantation of HIMs could also potentially indicate that people value privacy far less (or it could be interpreted as such) and, as Noah Feldman (Harvard law professor) argues, “the less we value it [privacy], the less our judicial institutions will protect it for us”.[686]

Although the ECPA regulates government access to stored electronic communications, communications from a tracking device is exempted from being included in electronic communications.[687] A “tracking device” is defined as “an electronic or mechanical device, which permits the tracking of the movement of a person or object”.[688] Both RFID and GPS implants are indeed types of tracking devices and, thus, may be explicitly excluded from the ECPA.

683 see *Kyllo v. United States*, 533 US 27, 34.

684 see Wood, David Murakami (ed.). A *Report on the Surveillance Society* (2006), p. 80.

685 Gossett, Sherrie. “Implantable-chip company in financial straits” (WorldNetDaily, 4 March 2003), available at: http://www.wnd.com/news/article.asp?ARTICLE_ID=31353

686 Feldman, Noah. “Strip-Search Case Reflects Death of American Privacy” (Bloomberg, 9 April 2012), available at: http://www.bloomberg.com/news/2012-04-08/strip-search-case-reflects-death-of-american-privacy.html

687 Title 18 U.S.C. Part I, Chapter 119, § 2510(12)(c).

688 Title 18 U.S.C. Part II, Chapter 205, § 3117(b).

In addition, relevant ***case law is not grounded on statutory law*** and the legal framework fails to provide adequate ***clarity*** and ***consistency***. While Rule 41 of the Federal Rules of Criminal Procedure requires that if law enforcement agents want to use or install a tracking device, they must obtain a warrant based on probable cause to do so, "[t]he traditional statutory framework governing electronic surveillance does not provide law enforcement with clear-cut guidance" (Clark, 2006, p. 25). The law does not clearly delineate whether or not probable cause or simply reasonable suspicion under Title 18 U.S.C Part I, Chapter 121 § 2703(d) is required for a warrant or court order requesting telecommunication companies to hand over cell-site information, whether historical, real-time or 'prospective', to government entities. Federal agencies are routinely asking US courts to order telecommunication companies to provide historical or real-time tracking/location data[689] and the basis of the decision to do so is at the discretion of judges (*Ibid*.), rather than based on explicit provisions in statutory law. The US Justice Department recommends that Federal prosecutors seek warrants based on probable cause, in order to access location information.[690] However, Federal judges differ as to whether the government actually requires probable cause to obtain a warrant to access the cell-site (location) information. Some judges have been granting warrants based not on probable cause, but rather based on considerable lower standards of suspicion (*Ibid*.). Local police officials are now also routinely using cell phones as a tracking tool "with little or no court oversight".[691]

Essentially, there is general disagreement whether or not location data gathered/obtained from cell phones/GPS-enabled smartphones/GPS tracking devices is protected by the Fourth Amendment and uncertainty about the procedures/requirements that law enforcement agencies must satisfy to access/use the location data, which has often enabled law enforcement agencies to access/use this data without probable cause or a warrant.

---

[689] As most recently revealed by the privacy activist Christopher Soghoian on his blog, Sprint Nextel provided law enforcement agencies with customer location data more than 8 million times between September 2008 and October 2009 made available through a web application developed by Sprint to handle the large volume of requests, according to a manager of the company, who disclosed the information at a non-public conference, available at: http://paranoia.dubfire.net/2009/12/8-million-reasons-for-real-surveillance.html

[690] Nakashima, Ellen. "Cell phone Tracking Powers on Request: Secret Warrants Granted Without Probable Cause" (Washington Post, 23 November 2007), available at: http://www.washingtonpost.com/wp-dyn/content/article/2007/11/22/AR2007112201444.html

[691] see Lichtblau, Eric. "Police Are Using Phone Tracking as a Routine Tool" (New York Times, 31 March 2012), available at: http://www.nytimes.com/2012/04/01/us/police-tracking-of-cellphones-raises-privacy-fears.html?_r=2&partner=MYWAY&ei=5065

Arguably, the US legal framework requires little or no evidence or degree of suspicion when tracking is destined to occur only in public places. As US Magistrate Judge James K. Bredar recognized, "[i]f acquisition of real-time cell site information is equivalent to a tracking device, it would seem the Government is not constitutionally required to obtain a warrant provided the phone remains in a public place where visual surveillance would be available".[692] Moreover, as US Magistrate Judge Gabriel Gorenstein pointed out, there is a difference between cell phones voluntarily carried and the Government's covert placement and use of tracking devices. HIMs are voluntarily implanted, at least for now. When an individual has chosen to voluntarily carry a device and permit the transmission of its information to a third party, the Fourth Amendment is not implicated.[693]

The same legal reasoning for cell phones and cell site information could apply to the use of GPS implants (and other GPS tracking devices) for law enforcement surveillance purposes when the implantee (or end-user) is in public (Ganz, 2005).[694] Equally, warrantless RFID tracking within public areas could also be considered lawful.

Already, a number of Federal courts that have deliberated on GPS tracking have extended the legal reasoning of the US Supreme Court in *United States v. Knotts* and *United States v. Karo* to the use of GPS tracking devices.[695] The 7th Circuit US Court of Appeals in *United States v. Garcia*, basing its decision on *Knotts*, upheld warrantless GPS tracking in public areas, denying that the use of a GPS tracking device constituted a search,[696] by incorrectly comparing the use of GPS satellites for vehicle tracking to the use of satellite imaging or CCTV cameras for observing a vehicle's route.[697] The 9th Circuit US Court of Appeals in *United States v. Pineda-Moreno* equally upheld that the use of a GPS tracking device by law enforcement agencies to monitor a person's

---

692 In the Matter of the Application of the United States of America for an Order Authorizing the Installation and Use of a Pen Register and a Caller Identification System on Telephone Numbers and the Production of Real Time Cell Site Information, United States District Court for the District of Maryland, Memorandum Opinion, 28 November 2005, p. 13.

693 see In Re Application of the United States of America for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace, United States District Court for the Southern District of New York, Opinion and Order, United States Magistrate Judge, Gabriel W. Gorenstein, 20 December 2005, p. 25.
The opinion is consistent with *Smith v. Maryland*, 442 U.S. 735, 744 (1979).

694 see Ganz, John S. I*t's Already Public: Why Federal Officers Should Not Need Warrants to Use GPS Tracking Devices* (95 The Journal of Criminal Law and Criminology, 2005).

695 see, e.g., United States v. Moran, 349 F.Supp.2d 425 (NDNY, 2005).

696 *United States v. Garcia*, 474 F.3d 994 (7th Circuit, 2007).

697 *Ibid.*, at 997.

movements in public is not considered a search under the Fourth Amendment and thus does not require a warrant.[698]

There are also a few State courts in the US that have clearly concluded that GPS tracking in public is not a search under the Fourth Amendment. For instance, the District IV Wisconsin Court of Appeals ruled that police are permitted to conduct warrantless GPS tracking, since the tracking does not constitute a search, as the law currently stands.[699] Interesting enough, the law's deficiency even caused the Wisconsin court to urge the state legislature to regulate police and private use of GPS tracking technology. In 2005, the Connecticut Appellate Court in *Turner v. American Car Rental, Inc* dismissed the intrusion upon seclusion tort claim, concluding that it was unaware of any legal precedent establishing that the installation of a GPS tracking device on a vehicle violates the privacy rights of the driver or that a driver has an expectation of privacy on a public highway.[700]

On the other hand, certainly not every US court agrees. The District of Columbia Circuit Court of Appeals in *United States v. Maynard*[701] reversed the drug conviction of Antoine Jones, which was significantly based on the location information gathered from a GPS tracking device installed on his vehicle without a warrant. The District of Columbia Circuit Court of Appeals held that warrantless GPS tracking violated the Fourth Amendment and that the location information obtained from the GPS tracking device was not public, concluding that Antoine Jones had a reasonable expectation of privacy of his movements. After the District of Columbia Circuit Court of Appeals overturned Jones' conviction, the Obama Administration petitioned the District of Columbia Circuit Court of Appeals to rehear the case *en banc*. The petition was denied.[702]

Some State courts have also ruled that GPS tracking requires a warrant. But, these decisions are premised on the respective State laws and State constitutions and not explicitly on Federal law or the Fourth Amendment,[703] and there were also compelling dissenting opinions.

---

698 *United States v. Pineda-Moreno*, 591 F.3d 1212 (9th Circuit, 2010).

699 *State v. Michael A. Sveum*, 769 N.W.2d 53, 59 (District IV Wisconsin Court of Appeals, 2009).

700 *Turner v. American Car Rental*, 884 A.2d 7 (Conn. App. Ct., 2005).

701 *United States v. Maynard*, 615 F.3d 544 (D.C. Circuit, 2010).

702 United States v. Jones, 625 F.3d 766 (D.C. Circuit, 2010).

703 see, e.g., *People v. Scott C. Weaver*, 12 N.Y. 3d 433, 435 (New York Court of Appeals, 2009); Washington v. Jackson, 150 Wash. 2d 251, 76 P3d 217 (2003).

However, since there are conflicting decisions in the US among the circuit courts concerning the constitutionality of warrantless GPS tracking under the Fourth Amendment, at the request of the US Government,[704] the US Supreme Court indeed granted a writ of certiorari in the case *US v. Jones* to potentially resolve and clarify the issue.[705]

It is important to point out that in *United States v. Knotts* the US Supreme Court ruled on RF tracking devices capable of enhancing the ability of law enforcement agents to conduct visual and physical surveillance, but the Court did not rule on GPS tracking capable of substituting or removing the need for visual or physical surveillance altogether, as both the EFF and ACLU highlight in their *amicus curiae* brief,[706] in support of the appellant in *US v. Jones* in the District of Columbia Circuit Court of Appeals.[707]

Moreover, the US Supreme Court also indicated in *United States v. Knotts* that other methods of more sophisticated electronic surveillance (i.e. GPS tracking) may require a different judgment[708] and in *Dow Chem. Co. v. United States* judged that satellite imaging may constitute a search under the Fourth Amendment, since it practically replaces, rather than enhances, the senses of law enforcement agents.[709] Indeed, using GPS devices to constantly track a person's movements for a prolonged period of time, replacing the need for law enforcement agents in the field, can divulge far greater amounts of data than using simple RF devices to assist law enforcement agents in the field when observing a person's movements for a limited period of time.

Furthermore, the District of Columbia Circuit Court of Appeals in *United States v. Maynard*[710] convincingly held that Antoine Jones' movements were actually not exposed to the public, since "the likelihood a stranger would observe all those movements is not just remote, it is essentially nil".[711] Indeed, the District of Columbia Circuit Court

---

704 Petition for a Writ of Certiorari, *United States v. Jones*, No. 10-1259 (April 15, 2011).

705 *US v. Jones*, USSC No. 10-1259, certiorari granted 6/27/11.

706 *Amicus curiae* literally means "friend of the court". According to Rule 37(1) of the Rules of the *Supreme Court of the United States (adopted 17 July 2007), an amicus curiae* brief "brings to the attention of the Court relevant matter not already brought to its attention by the parties may be of considerable help to the Court".

707 see Brief of *Amici Curiae* Electronic Frontier Foundation and American Civil Liberties Union of the National Capital Area in Support of Appellant Jones, 3 March 2009.

708 *United States v. Knotts*, 460 U.S. 276, 283-284 (1983).

709 *Dow Chem. Co. v. United States*, 476 U.S. 227, 238-239 (1986).

710 *United States v. Maynard*, 615 F.3d 544 (D.C. Circuit, 2010).

711 *Ibid*., at 560.

of Appeals made a strong argument in differentiating between the tracking of a vehicle's single journey and the prolonged, non-stop tracking of a vehicle. Emmett (2011) agrees with this argument.[712]

But, as the US Government contends, the US Supreme Court in *Knotts* did not make this distinction.[713] In addition, as the US Government also points out, the US Supreme Court in *United States v. Karo* did not judge that the length of time or duration was a factor in determining whether or not electronic tracking constituted a search under the Fourth Amendment.[714]

Up until 2011, the US Supreme Court had not yet had an occasion to deliberate on the legal questions concerning GPS tracking or to judge whether or not the installation and use of GPS tracking devices constitutes a search under the Fourth Amendment. Since the US Supreme Court has granted a writ of certiorari in the case *US v. Jones*,[715] this occasion finally arrived.

The US Supreme Court, in *United States v. Jones*, ended up ruling against the US Government (and some previous circuit court decisions), judging that the installation and use of a GPS tracking device to monitor the movements of a vehicle constitutes a search within the meaning of the Fourth Amendment (i.e. concurring with the District of Columbia Circuit Court of Appeals). But, as earlier predicted (see, e.g., Ganz, 2005), the Court did not explicitly rule that GPS tracking requires a warrant. Although, the minority concluded in their separate opinions that prolonged GPS tracking/monitoring could amount to a search requiring a warrant, the majority declined to decide whether or not the search in this specific case required a warrant. The Court argued that it was not required, in this particular case, to clarify whether or not electronic monitoring (i.e. GPS tracking/monitoring) for prolonged periods of time is an unconstitutional invasion of privacy or to judge whether this type of search was reasonable or unreasonable. As a result of procedural rules, the majority considered that argument *forfeited*.

712 For example, Emmett (2011) argues: "Close consideration of both the duration of the electronic monitoring and the GPS technology that enabled the surveillance would have revealed that law enforcement obtained information of a type that was not available to the public through simple
(or even technologically enhanced) visual surveillance" (Emmett, Caitlin. *United States v. Pineda-Moreno, Tracking Down Individuals' Reasonable Expectation of Privacy in the Information Age* (41 Golden Gate University Law Review, 2011), p. 26.

713 Petition for a Writ of Certiorari, *United States v. Jones*, No. 10-1259 (U.S. Apr. 15, 2011), p. 14.

714 *Ibid*., p. 15.

715 *US v. Jones*, USSC No. 10-1259, certiorari granted 6/27/11.

Given the conservative majority of the current US Supreme Court,[716] the Court, as a result, neither contradicted *United States v. Karo*, which held that evidence or probable cause is not required to observe information conveyed in areas observable to the public,[717] nor backpedaled on a landmark decision with regards to RF tracking in *United States v. Knotts*. On the contrary, these decisions were essentially reaffirmed.

Moreover, in light of the US Supreme Court's decision in *Kyllo v. United States*, which judged that the greater availability and more widespread the deployment and adoption of a particular technology the less reasonable expectation of privacy the public enjoys with respect to its use,[718] the widespread availability of GPS tracking devices and the widespread use of GPS technology has significantly reduced the reasonable expectation of privacy of one's movements in public. Now that GPS tracking has already become a common practice in criminal investigations, this legal interpretation has only been amplified.

Therefore, the legal matter is still not closed and the conflicting decisions among the circuit courts are not fully settled. There is, as a result, no compelling way to foresee how the US Supreme Court, or other US courts, will rule on future warrantless GPS (or RFID) tracking cases. Essentially, the law, as it stands now, arguably still fails to provide ***foreseeability, consistency*** and ***clarity***, regarding the use of tracking technologies by law enforcement agencies.

Unless significant changes manifest in the near future, in light of the relevant case law, the vacuum of law, the US Government's warrantless wiretapping controversy, the increasing abuse of the National Security Letters process, the revealed "President's Surveillance Program" [referring to former US President George W. Bush], the PATRIOT Act, the Protect America Act of 2007, which amended the Foreign Intelligence Surveillance Act (FISA) and removed the warrant requirement for government surveillance of international electronic communications, the increasing use of cell phones for real-time tracking and the increasing availability and widespread use of GPS technology, the signs are there that warrantless GPS tracking will only further develop as a common practice. Accordingly, there is still increasing pressure from the US Government to allow for warrantless GPS tracking.

---

716 For further discussion and analysis on the increasingly conservative judgments of the US Supreme Court, see Chemerinsky, Erwin. T*he Conservative Assault on the Constitution* (Simon & Schuster, 2010).

717 *United States v. Karo*, 468 U.S. 705 (1984).

718 see *Kyllo v. United States*, 533 U.S. 27, 34 (2001).

In short, as a consequence of the legal deficiencies and dilemmas outlined above, the examination by law enforcement agencies of the location information generated by both RFID and GPS implants is, at present, not granted Fourth Amendment protections.

Moreover, in light of the recent *Hiibel v. Sixth Judicial District Court of Nevada,* 542 U.S. 177 (2004) decision, which held that police may oblige a person to provide identification upon request when conducting an investigation, the reading of a person's RFID implant, which constitutes a form of identification, may also arguably not constitute a search under the current legal framework (Herbert, 2006).

Furthermore, since the printouts of location information generated by GPS and RFID tracking may be considered originals and due to the interpretation of the Fifth Amendment, as it stands now, the location information pertaining to HIMs could be used as potentially incriminating evidence in a court of law. The apparent ***lack of foreseeability*** and ***clarity*** of Fourth Amendment interpretations of electronic tracking in public, or the lack of specific Federal statutory rules concerning the use of or access to location information generated by RFID/GPS implants, may also quash the possibility of resorting to the 'exclusionary rule'.

When it comes to the private sector, tort law is equally not applicable to the location information generated by HIMs, as the current US legal framework stands, since it is generally accepted by courts in the US that "there is no liability for giving further publicity to what the plaintiff himself leaves open to the public eye", as elaborated in the comments of the Restatement (Second) of Torts.[719] Hence, as McClurg (1995) rightfully points out, the problem is not so much with the definition of the tort of intrusion, but rather the Restatement comments pertaining to that definition. As McClurg (1995) further points out, the adherence of US courts to the outmoded rule and viewpoint that privacy and seclusion, for the most part, cannot be intruded upon in public places exhibits a deficient understanding of the purpose of privacy and the other civil liberties it is meant to defend. An additional problem with tort of intrusion of privacy, as Schwartz (2000) points out, is that the intrusion must be "highly offensive"[720] and that case law has shown that most stealthy intrusions are unlikely to be found sufficiently "objectionable" (Schwartz, 2000, p. 778).

Significantly, the US legal framework is ***not up to date*** with the current technology. While there is no explicit Federal law that regulates the privacy implications of RFID or

---

719 Restatement (Second) of Torts, § 652D, comment b (1977). see, e.g., *Hartman v. Meredith Corp.*, 638 F. Supp. 1015, 1018 (D. Kan. 1986) ("The plaintiffs must show that there has been some aspect of their private affairs which has been intruded upon and does not apply to matters which occur in a public place or place otherwise open to the public eye").

720 Restatement (Second) of Torts, § 652B.

the information collected and stored as a result of RFID technology, there are equally no specific statutes or regulations that sufficiently address the privacy implications of GPS tracking. Although Federal law regulates the disclosure of location information generated by cell phones (as part of CPNI), and also regulates governmental access to private/stored electronic communications, the law, however, does not apply to the location information generated by RFID or GPS implants. As Reneger points out, the Telecom Act "offers no protection for people whose privacy is violated through non-cell-phone-based collections of location information" (Reneger, 2002, p. 562). Herbert similarly agrees that while cell phone users may have a reasonable expectation of privacy of their call location information, "non-cellular forms of wireless products containing GPS technology are not currently protected by any statutory location privacy protections" (Herbert, 2006, p. 445). Moreover, the meaning of location information is explicitly restricted to "call location information concerning the user of a commercial mobile service",[721] and therefore does not cover the more extensive location information generated by HIMs or other similar PLDs. Consequently, with the exception to the CPNI of cell phones, as the law stands now, location information generated by devices other than cell phones is not afforded adequate privacy protection. This deficiency may be partly the result of the US piecemeal legal approach to protecting privacy, which is particularly sectoral rather than all-inclusive or comprehensive.

Under the US legal framework, "telecommunications carriers" are defined as "any provider of telecommunications services".[722] RFID or GPS implants could only come into the scope of the Telecom Act if companies like Digital Angel, ADS or VeriChip Corp. (now known as PositiveID), for example, were considered telecommunications carriers, commercial mobile service providers or joint venture partners. However, none of these companies are considered as any of these types of entities. As a result, there are arguably little or no legal barriers, at present, that prevent companies, like ADS or Digital Angel, from selling location information generated by HIMs to third parties.

One of the other main dilemmas is that the US legal framework does not have comprehensive, cross-sectoral privacy legislation equivalent to the EU's Data Protection Directive,[723] which is binding on both private entities and public authorities (except

[721] Title 47 U.S.C. Chapter 5, Subchapter II, Part I, § 222(f).

[722] Title 47 U.S.C. Chapter 5, Subchapter I, § 153(44). "Telecommunications" are defined as the "transmission, between or among points specified by the use, of information of the user's choosing without change in the form or content of the information sent and received". Title 47 U.S.C. Chapter 5, Subchapter I, § 153(43).

[723] Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

for law enforcement agencies). The EU's Data Protection Directive even affects entities without activities or operations in the EU, since the Directive regulates the transfer of personal data from EU Member States to any third party outside the EU. Article 25 requires that personal data from the EU must not be transferred to any country outside the EU unless that country has "adequate" privacy protections. A conflict between the US and EU over whether or not privacy laws in the US were adequate or up to par with the EU's Data Protection Directive may have arguably resulted in the US-EU 'Safe Harbor' arrangement, in order to alleviate some of the differences, whereby US companies voluntarily self-certify their adherence to the safe harbor requirements or participate in a self-regulatory organization that adheres to the requirements. However, the need for the 'safe harbor' agreement in the first place only revealed an agreement that the US legal framework, in terms of privacy protection, is relatively weak and inadequate in comparison to the EU legal framework.

Instead of comprehensive privacy legislation, the US relies on a hodgepodge of a number of statutory laws covering separately different sectors or themes. But, as Reidenberg argues, "sectoral regulations are reactive and inconsistent" and the "gap-filling approach also leaves many areas of information processing untouched and runs counter to the cross-sectoral nature of modern data processing" (Reidenberg, 2000). Indeed, none of the US sectoral laws, for instance, can be applied adequately to RFID applications.

On the other hand, the EU's Data Protection Directive (Directive 95/46/EC) does apply to the processing of personal data by RFID technology.[724] Nevertheless, even though the EU has far superior privacy law, the EC has recognized that there are indeed difficulties in applying the Data Protection Directive to new technologies, even if the Directive is meant to be technologically neutral or independent. The EC has further recognized that it may be necessary to develop additional specific provisions or new legislation to defend against the new threats posed by RFID and other technological developments.[725] The EU plans to replace the Data Protection Directive with a General Data Protection Regulation, and is considering the formulation of specific legislation or *lex specialis*, with respect to

---

[724] The EU's Article 29 Working Party on data protection has established that the Data Protection Directive strictly applies to the personal data collected through RFID and that the data protection principles should be implemented within RFID technology. see Article 29 Working Party, Working document on data protection issues related to RFID technology, January 2005 (WP 105).

[725] see Com (2007) 87 final, Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive.

the Data Protection Directive, to address the special privacy issues surrounding RFID.[726] The EC also felt that there was a need to specify that the 'ePrivacy Directive'[727] explicitly applies to RFID.[728] The EC has also adopted a set of recommendations to ensure the protection of privacy and personal data in applications supported by RFID technology,[729] but the recommendations are more focused on RFID applications used in retail trade activities.[730]

---

726 see Commission Staff Working Document, Accompanying document to the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Future networks and the Internet: Early Challenges regarding the "Internet of Things", p. 8; COM(2007) 96 Final, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Radio Frequency Identification (RFID) in Europe: steps towards a policy Framework, available at: http://ec.europa.eu/information_society/policy/ecomm/doc/library/proposals/dir_citizens_rights_en.pdf

727 Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector.

728 see COM(2007) 698 final. Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation, p. 19, para. 28; see Directive 2009/136/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009, recital 56. Accordingly, Article 3 of the ePrivacy Directive, which defines the scope of the directive, was revised to include "*public communications networks supporting data collection and identification devices*". The amendments ensure that the EU's data protection legal framework covers RFID. For further discussion, see Cannataci, Joseph A. *Recent developments in privacy and healthcare: Different paths for RFID in Europe and North America?* (International Journal of RF Technologies, Volume 2, 2010/2011), pp. 173–187.

729 C(2009) 3200 final, Commission Recommendation of 12.5.2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification.
The recommendation calls for a PIA framework for RFID. The European Commission will later analyze the impact of the recommendation on companies, public entities and citizens (Cannataci, 2011). If the impact is adequate, then perhaps specific rule-making for RFID applications may be put aside (Cannataci, 2011).

730 I attended the 3rd closed meeting of the RFID Recommendation Implementation Informal Working Group at the EC. Present at the meeting were industry associations, standardization bodies, public authorities and a representative from the Article 29 Working Party. The first goal of the group was to establish an agreed upon generic pan-European PIA Framework for RFID applications (RFID PIA) with the endorsement of the Article 29 Working Party. This was accomplished in February 2011. The ultimate seal of approval came in April 2011, when the RFID PIA was officially signed by the European Commission Vice President (Neelie Kroes), the Chairman of the Article 29 Working Party (Jacob Kohnstamm), the Executive Director of the European Network and Information Security Agency (Udo Helmbrecht) and various retail and RFID industry representatives, including GS1 and the European Retail Round Table (For further information/explanation, see Cannataci, 2011). The RFID PIA framework is the first of its kind in Europe, and supplementary templates and checklists are to be developed for specific RFID applications. It is important to point out that while the RFID PIA framework is a step in the right direction, the main problem is that it will only be applicable to RFID application service providers, and not to the developers of RFID infrastructures/systems. This is, unfortunately, consistent with the Data Protection Directive.

In addition, the EC has also recognized the opinion of the European Group on Ethics (EGE) that "non-medical ICT implants [HIMs] in the human body are not explicitly covered by existing legislation, particularly in terms of privacy and data protection".[731] The EGE recommended that the EC initiate legislation on HIMs.[732] Surely, without equally comprehensive privacy legislation, the US legal framework is in far worse shape and, above all, requires specific legislation on RFID, let alone for HIMs.

Since there is no Federal law yet on RFID technology whatsoever, there is also essentially a lack of legal consistency concerning RFID in the US, as the relatively few existing State laws on RFID vary considerably in substance, scope and purpose. Most of the State laws address the use of RFID tags embedded in retail products or identity documents. Moreover, some of the State laws that address RFID technology are insufficient and are not without their own flaws. For example, in Washington, the State law criminalizes the unauthorized reading of an RFID identification device, "for the purpose of fraud, identity theft, or for any other illegal purpose", as a class C felony.[733] Thus, this law only prohibits reading an individual's RFID identification when it is done so for illegal purposes and does not prohibit the reading for identification and tracking purposes alone. Nevertheless, as EPIC Executive Director Marc Rotenberg pointed out in a prepared testimony before the House of Representatives Oversight Committee's Information Policy, Census and National Archives Subcommittee, the US Government typically acts only after the identity theft has occurred.[734]

However, while there is no Federal statutory law clearly regulating the use of GPS tracking devices, some states, such as California, have statutory laws regulating the activity. California Penal Code Section 637.7 (a) mandates: "No person or entity in this state shall use an electronic tracking device to determine the location or movement of a person". But, this law is clearly only applicable to persons in vehicles, and therefore does not explicitly cover GPS tracking via smartphones or GPS implants. For instance, Subsection (b) states: "This section shall not apply when the registered owner, lesser, or lessee of a vehicle has consented to the use of the electronic tracking device with respect to that vehicle". Moreover, Subsection (d) defines an "electronic tracking device"

---

[731] Opinion of the European Group on Ethics in Science and New Technologies to the European Commission, Opinion No. 20, Adopted on 16/03/2005, Section 6.5.4.

[732] *Ibid.*

[733] see Title 19, Chapter 19.300, § 19.300.020.

[734] see Marc Rotenberg's prepared testimony, available at: http://informationpolicy.oversight.house.gov/documents/20090617111417.pdf

as "any device attached to a vehicle or other movable thing that reveals its location or movement by transmission of electronic signals".

Moreover, although state legislatures in the US have also enacted breach notification laws concerning personal data, there is no Federal law yet,[735] which would be ideal for any nationwide breach and for establishing common notification standards. Instead, state laws can vary somewhat on the process behind the notification of breaches.

The DHS claims that the Privacy Act 1974 regulates the data collected through RFID, stating the following:

> When RFID is used for <u>human tracking</u>, the data collected will undoubtedly comprise a "system of records" under the Privacy Act of 1974. People should have at least the rights accorded them by that law when they are identified using RFID. Systems using RFID technology are, of course, also subject to the E-Government Act's Privacy Impact Assessment [PIA] requirements[736] (emphasis added).

The Privacy Act 1974 does not restrict the content of a "record" to education, financial transactions, medical history and criminal or employment history and may indeed be applicable to data collected through RFID technology. However, in accordance with the current legal standpoint of jurisprudence in the US, concerning the absence of privacy while in public, and the lack of legal clarity concerning the privacy of location information, the Privacy Act 1974 arguably may not be applicable to the location information collected via RFID implants/microchips and RFID readers in public spaces. If the US legal

---

735 Senator Patrick Leahy recently introduced S.1490, entitled "the Personal Data Privacy and Security Act of 2009", which could have provided for a national standard for data breach notification. More recently, the Secure and Fortify Electronic Data Act (the "SAFE Data Act") was proposed in the US House of Representatives, which aims to establish Federal (i.e. nationwide) breach notification requirements, overriding all existing state breach notification laws. With the recently adopted EU Telecom Package and revision of the 'ePrivacy' Directive, the EU has already passed laws requiring communications service providers to notify consumers of security/data breaches. see Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector; Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.

736 The Use of RFID for Human Identification: A Draft Report from DHS Emerging Applications and Technology Subcommittee to the Full Data Privacy and Integrity Advisory Committee, Version 1.0, p. 4, available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_rpt_rfid_draft.pdf
This statement was partially amended in the final version. Instead of writing "when RFID is used for human tracking", the final version writes "when an RFID-enabled system is used to collect data about individuals". see The Use of RFID for Human Identify Verification, Report No. 2006-02, Data Privacy & Integrity Advisory Committee, Adopted 6 December 2006, p. 4, available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf

framework does not prohibit the use of location information obtained by law enforcement agencies via GPS tracking devices without a warrant, it would be hard to imagine how the US legal framework would effectively regulate or prohibit the use of location information generated and transmitted to third parties via HIMs voluntarily implanted.

Nevertheless, even if the Privacy Act 1974 is somehow interpreted to be applicable in regulating the storage/processing of location information collected through RFID readers placed in the public space, this is only possible for the location information collected, stored and used by the US Government. The Privacy Act 1974 is only applicable to agencies and the term "agency" is specifically defined as:

> any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency.[737]

Therefore, the Privacy Act 1974 is in no way applicable to HIM service providers, which may store the location information generated by HIMs, or any other private data controller for that matter. Moreover, the Privacy Act 1974 does not prohibit the US Government from buying vast quantities of personal information from commercial data brokers, which is in fact an ongoing trend.

Privacy Impact Assessments (PIAs)[738] may be required to evaluate how personal information in identifiable form will be collected, maintained and disseminated using RFID, however, this is also only applicable to personal information held (and technologies/systems used) by the US Government (i.e. Federal public agencies). A PIA was in fact conducted regarding RFID technology, but this specifically pertained to RFID tags embedded in government documents, and not the general use of RFID technology for other applications. Moreover, as Cannataci highlights, PIAs in the US are not being used to induce the implementation of technical measures to safeguard privacy (2011, p. 182).

In addition, the US legal framework, pertaining to privacy protection, ***relies primarily on private sector self-regulations*** (privacy policies, voluntary standards or codes of conduct), whereby self-regulations and internal self-reporting are often preferred over

---

[737] Title 5 U.S.C. Part I, Chapter 5, Subchapter II, § 552(f).

[738] In US law, a PIA is described as "an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks" (E-Government Act of 2002, Section 208).

'hard' laws and (external) scrutiny. Moreover, the US approach to privacy protection generally promotes the view that self-regulations are friendlier towards the freedom of information and commerce and the promotion of innovation. The rationale behind this may be based on the laissez-faire economic theory, whereby the belief is that the market usually ends up regulating itself. While there are indeed a number of examples of this rationale proving true, such as the controversy surrounding the unveiling of Intel Corporation's Pentium III microchip in January 1999 (Werner, 2008),[739] there are plenty of more examples proving it to be untrue.

Self-regulations or codes of conduct, without the existence of binding 'hard' laws to establish the minimum standards as their basis, can barely be considered reliable. Consumers/citizens especially cannot depend on self-regulations/codes of conduct when the self-regulations are themselves insufficient and stagnant and cater to the self-interests and requests of major industry players. The over-reliance solely on self-regulations may result in requirements guided by the "invisible hand", not requirements imposed by transparent, binding laws. This approach raises concerns of ***the lack of accountability*** and supervision. The same mistake of over-relying on investment banks and other financial institutions to self-regulate the risky financial derivatives market was made over the last decade and we have now witnessed the enormous negative consequences of that system. This approach is not relied upon or trusted for regulating product safety or the use of chemicals, and there is also little reason it should be relied upon or trusted for safeguarding privacy.

Self-regulations have proved to be insufficient to address threats to privacy. For instance, Schwartz (1999) rightfully argued early on that industry self-regulations are inadequate to regulate online privacy. As EPIC later showed, self-regulations indeed have seriously failed to provide online privacy and regulate the use of cookies.[740] Self-regulations have also failed to ensure the appropriate content and availability of privacy policies for social networking websites.[741] The World Privacy Forum has also highlighted that self-regulation initiatives (e.g. the Networking Advertising Initiative) have been

---

[739] The original design for Intel's processor microchip had a serial number embedded within the hardware code that could enable online marketers to identify and track Internet users. Consumer boycott threats led to Intel removing the identification system. see Clausing, Jeri. "Intel Alters Plan Said to Undermine PC User's Privacy" (New York Times, 26 January 1999), p. Al; Werner, Matthew. Google and Ye Shall Be Found: Privacy, Search Queries, and the Recognition of a Qualified Privilege (34 Rutgers Computer & Technology Law Journal 313, 2008).

[740] Jay Hoofnagle, Chris. *Privacy Self Regulation: A Decade of Disappointment*, EPIC, 4 March 2005, available at: http://epic.org/reports/decadedisappoint.pdf

[741] see Bonneau, Joseph and Sören Preibusch. *The Privacy Jungle: On the market for data protection in social networks* (WEISS, 2009).

inadequate to defend consumer's privacy against online targeted behavioral advertising technologies.[742] As a result of the failures, EPIC recommended that the FTC "should abandon its faith in self-regulation", concluding that "[s]elf-regulatory systems have served to stall Congress while anesthetizing the public to increasingly invasive business practices".[743]

Unfortunately, however, with regards to RFID, the US Government regrettably believes, for now at least, that self-regulations are sufficient to regulate RFID. Some at the FTC have concluded that "technology-specific privacy legislation is unnecessary at this juncture" regarding RFID.[744] But, self-regulations are obviously only effective to the extent to which companies comply. While, in the US, Better Business Bureaus can be leveraged to help put into effect self-regulations, this approach relies on voluntary compliance. Moreover, while the FTC has the authority to enforce a company's privacy policy/code of conduct, no rights of private legal action are available under the FTC Act. Therefore, it may also be unrealistic to claim that the current approach adequately satisfies the ***principle of enforcement/redress***.

Without comprehensive privacy legislation in the US or Federal statutory laws that explicitly regulate HIMs and protect or restrict access to location information generated by them, we are left to rely on the self-regulations and good will of companies like ADS/Digital Angel and VeriChip Corp. However, companies, such as Digital Angel or VeriChip Corp., can gain considerably from selling location information. Moreover, the privacy policy of VeriChip Corp., like with other US companies, is subject to changes.[745] As VeriChip Corp. themselves previously declared, "[w]e reserve the right

---

[742] World Privacy Forum, "The Network Advertising Initiative: Failing at Consumer Protection and at Self-Regulation", November 2007.
But, this did not at all prevent the FTC from doubling down on its self-regulation policies, which later published the FTC Staff Report, "Self-Regulatory Principles For Online Behavioral Advertising: Tracking, Targeting, and Technology" (February 2009).
Hirsch has equally highlighted that the reliance on self-regulations and the Network Advertising Initiative to control the use of online targeted advertising has been largely unsuccessful or ineffective. see Hirsch, Dennis. *Law and Policy of Online Privacy: Regulation, Self-Regulation or Co-Regulation* (Seattle University Law Review, Vol. 34, Issue 2, 2011), pp. 439-480.
The industry association, Digital Advertising Alliance, also adopted in 2010 a "Self-Regulatory Program for Online Behavioral Advertising", but its success is equally questionable.

[743] Jay Hoofnagle, Chris. *Privacy Self Regulation: A Decade of Disappointment*, EPIC, 4 March 2005, available at: http://epic.org/reports/decadedisappoint.pdf

[744] FTC staff report on RFID, p. 20.

[745] For instance, Facebook is constantly changing its privacy policies.

to change our Privacy Policy".[746] Although ADS/Digital Angel proclaims their policy now is not to release the data they collect to third parties, their policy was different before. As Edmundson (2005) reveals, the privacy policy of Digital Angel (formerly a major shareholder of VeriChip Corp.), which was previously available on their corporate website, actually stated, in contrary, that "[w]e [Digital Angel] may, from time to time, share, sell or rent some of your personal information with third parties with who we have a business relationship […]".[747]

The AMA's Code of Ethics, the GIS Code of Ethics, the proposed creation of geo-location standards by W3C, and other self-regulations or industry guidelines, as significant as they may be, are not a valid replacement for legally binding 'hard' laws enforceable in a court. Other privacy guidelines on RFID, such as CTIA's Best Practices and Guidelines for Location Based Services, do not cover RFID technology, and the RFID Privacy Guidelines developed by the Center for Democracy and Technology do not even mention human-implantable RFID microchips.

Although the FDA determined that VeriChip's RFID implants are regulated medical devices, in accordance with the Section 201 (h)(2) of the Federal Food, Drug and Cosmetic Act (FD&C Act), "when marketed [intended] to provide information to assist in the diagnosis or treatment of injury or illness",[748] they are *not* regulated medical devices with regards to their intended uses for security, financial and personal identification purposes.[749]

Essentially, without a federal law specifically stipulating otherwise, the legal framework may be potentially inadequate to ensure that HIMs are only implanted voluntarily and, therefore, may fail to uphold the ***principle of consent***. Indeed, RFID implants are implanted into the body using a syringe and, therefore, forced implantation should naturally be considered a violation of the right to bodily integrity, as Ramesh (1997) rightfully points out.[750] The Fourth Amendment, Fifth Amendment and even potentially the Thirteenth Amendment of the US Constitution, as Herbert argues, including the Equal Protection Clause and Due Process Clause, should also put a stop to forced im-

---

746 see VeriChip Corp., available at: http://www.verichipcorp.com/content/company/privacy

747 Edmundson, Kristen E. *Global Positioning System Implants: Must Consumer Privacy Be Lost in order for People to be Found* (38 Indiana Law Review 207, 2005), pp. 207-238, at: 215-216.

748 see a letter written by David E. Troy, Chief Counsel for the FDA, to Jeffrey N. Gibbs, a lawyer representing ADS, in 17 October 2002, available at: http://www.fda.gov/ohrms/dockets/dailys/03/dec03/120503/81n-0033p-sup0003-vol86.pdf

749 *Ibid.*

750 see Ramesh, Elaine M. *Time Enough? Consequences of Human Microchip Implantation*, Franklin Pierce Law Center (1997) available at: http://www.fplc.edu/risk/vol8/fall/ramesh.htm.

plantation (Herbert, 2006). Moreover, the liberty-based approach in the US to privacy would also strongly oppose the mandated implantation of HIMs.[751]

However, although the right to bodily integrity is clearly established by the US Constitution and case law, forced vaccinations, termed "countermeasures", are nevertheless considered lawful, in accordance with the Homeland Security Act of 2002, when the US Government issues a declaration asserting that the occurrence of "an actual or potential bioterrorist incident or other actual or potential public health emergency".[752] Already forced flu and pneumococcal vaccinations on young children in New Jersey were previously approved by the state's Public Health Council. With past precedence and the necessary laws enacted, if the H1N1 virus (also known as the "swine flu") does in fact become a genuine pandemic, forced vaccinations nationwide are therefore not farfetched (at least it was previously not farfetched during 2009), especially for nurses, teachers, etc. While travelling to some countries requires travelers to be vaccinated beforehand and some universities in the US (e.g., the University of Alabama) could mandate that students must be vaccinated before being allowed to enroll, this is more of a condition of exercising a privilege, rather than mandatory vaccination.

With numerous other threats to security, the US Government could also possibly invoke the changing standard of what is considered a 'reasonable' infringement of privacy as the potential basis of the mandatory implantation of HIMs for certain categories of people, if, for example, crime reached epic proportions or if there was another major terrorist attack. As Herbert (2006) further argues, in light of legal jurisprudence, while GPS bracelets are less intrusive than HIMs, this does not necessarily mean US courts will rule HIMs to be anymore unreasonable under the Fourth Amendment than GPS bracelets (Herbert, 2006, pp. 442-43).

Moreover, with regards to stalking, the laws in several states, as pointed out by Miller (2001), have provisions that restrict their applicability.[753] In North Carolina, for example, stalking refers only to instances where the stalker follows or is in the physical presence of the victim[754] and in Maryland the State law defines stalking in terms of

---

751 For further discussion, see Whitman, James. *Two Western Cultures of Privacy: Dignity Versus Liberty* (113 Yale Law Journal 1151, 2003).

752 see Public Law 107-296, Section 304.

753 see Miller, Neal. *Stalking Laws and Implementation Practices: A National Review for Policymakers and Practitioners* (2001), p. 36, available at: http://www.ncjrs.gov/pdffiles1/nij/grants/197066.pdf

754 see *N.C. Gen. Stat.*, § *14-277.3*.

approaching or pursuing a person.[755] Since then, state and federal laws have provided for stalking by means of telecommunication devices. However, while federal law now covers cyberstalking or stalking using electronic devices, the law is only applicable when the stalker or perpetrator has threatened, harassed or intentionally annoyed another person (Miller, 2001). Therefore, stalking laws are arguably not applicable to the use of telecommunication/electronic communication devices to purely track or monitor the movements of another person using electronic or digital means (Miller, 2001).

Furthermore, the law, at present, is *neither anticipatory of the further advancement of the technology* in the very near future. Today, a separate legal framework is more or less applied for the information society/virtual world and the physical world. However, as the physical world and virtual world are more and more merged or 'bridged' so to speak, due to the potential of an 'Internet of Things' and an 'Internet of Persons', this separation is deficient and increasingly no longer valid.

In summary, in light of the above legal deficiencies and dilemmas, the law, as it stands now, is unable to adequately protect the privacy and civil liberties of implantees, uphold the Fourth Amendment and Fifth Amendment, ensure privacy against the intrusive capabilities of HIMs or other PLDs, provide for the reasonable privacy of location information in an age of increasing location-awareness, and permanently guarantee the voluntary implantation of HIMs.

7.10 RECOMMENDATIONS ON ENHANCING THE US LEGAL FRAME WORK

As US Vice President Joseph Biden (then US Senator) notably expressed, when listing potential landmark decisions for the 21st Century, during the US Supreme Court confirmation hearings for Justice John Roberts in September 2005:

> Can a microscopic tag be implanted in a person's body to track his every movement? There's actual discussion about that. You will rule on that — mark my words — before your tenure is over.[756]

---

[755] see *Md. Code* Ann., art. 27, §*124*.

[756] "Transcript: Day One of the Roberts Hearings" (Washington Post, 13 September 2005), available at: http://www.washingtonpost.com/wp-dyn/content/linkset/2005/09/14/LI2005091402149.html

However, once again, if we adopt the "originalist" or "textualist" approach to understanding the US Constitution, then entirely new laws should be adopted, when deemed necessary, by elected legislators/representatives. Therefore, instead of relying on the US Supreme Court to judge in the future (sometime in the next 10-15 years) on the legality of HIMs and to finally rule on the legality of prolonged, widespread electronic tracking of individuals or to clarify the definitive standard for the US Government to be permitted to access location information, the US Congress should proactively formulate and adopt comprehensive Federal legislation. Specific laws for HIMs and location information would eliminate the excessive dependence on US courts to fill in the legal vacuum with altering and opposing judicial interpretations. After all, the legislative branch, once again, is meant to create law, as opposed to the judicial branch, which is principally meant to apply it. Besides, as outlined earlier, based on the relevant legal precedent, it may be unfavorable, in this case, to solely rely on the US Supreme Court.

Nevertheless, it will probably take at least 15 years or more and the widespread deployment of HIMs before the US Congress adopts comprehensive legislation regulating HIMs. As Herbert argues, "[t]he lack of substantial legislative movement in the field of tracking technology renders it unlikely that there will be a federal legislative response to human implants in the near future" (2006, p. 443). Moreover, as Herbert further points out, "it is far more probable that a majority in the current [109^{th}] Congress will continue to defer to the marketplace for potential corrective action aimed at avoiding privacy intrusions" (2006, p. 413). This is consistent with the overall US policy and approach to privacy protection, whereby legislation is adopted only after the privacy threat becomes serious. It is also consistent with the arguably mistaken belief that regulations are still premature for RFID applications.

Legislation should establish specific privacy safeguards to counter the serious threats to privacy posed by both RFID and GPS technology, particularly in the wake of HIMs being developed and deployed. Still, such legislation should also be comprehensible and flexible enough, and thus applicable to location information regardless of the technology (system, device, etc.) used, and to all entities and services that generate or require access to location information. With a flexible approach, LBS, location-aware applications and human tracking activities are broadly covered in an increasing location-aware world. Nevertheless, the legal rules for HIMs will need to be particularly more restrictive and precise than, for example, the use of a GPS tracking device by an employer in a company-owned vehicle to track their employees only during working hours (Herbert, 2006) or the use of a tracking device in a rented vehicle.

There have been a number of attempts to pass federal legislation regulating RFID. For instance, in 2004, the Opt Out of ID Chips Act[757] was introduced in the US House of Representatives, but ended up being unsuccessful. Although federal legislation on regulating RFID has suffered strong opposition, there are exceptional supporters within the US Congress.[758] There have also been attempts to pass legislation to regulate and protect the privacy of location information in general.[759]

Specific laws, regulations and adaptations in the legal framework are required to safeguard privacy against the threats posed by HIMs and other location-based services. These laws and regulations will not necessarily thwart innovation or commerce pertaining to RFID and GPS. On the contrary, specific laws and regulations could facilitate further development and deployment, ensuring the consumer confidence and trust necessary to open the market to the array of security and commercial benefits HIMs, and other RFID and GPS applications, can indeed provide.[760] Without specific federal regulations, both the private and public sector will face public opposition from all directions to the widespread deployment of HIMs. As RAND Europe equally asserts, the lack of specific mandates is an obstacle to the further deployment of RFID, suggesting that legislation, supported by public information campaigns, will address the privacy concerns and uncertainties of the general public towards RFID.[761] The uncertainties of the scope of data protection rules and the concept of personal data are also a main cause of regulatory uncertainty for industry players and investors in RFID applications, as revealed by the 2006 RFID public consultation in Europe.[762] Still, there are those who

---

[757] H.R. 4673, 108th Congress (2004).

[758] US Senator Patrick Leahy, a consistent defender of privacy, has persistently warned that RFID technology must be federally regulated and has called for congressional hearings on the technology. see Remarks of US Senator Leahy, "The Dawn of Micro Monitoring: Its Promise, and Its Challenges to Privacy and Security," Conference On "Video Surveillance: Legal And Technological Challenges", Georgetown University Law Center, 23 March 2004, available at: http://leahy.senate.gov/press/200403/032304.html

[759] see S.1164, The Location Privacy Protection Act of 2001, Section 2, introduced unsuccessfully by former US Senator John Edwards during the 107th session of Congress.

[760] I sent an email to VeriChip's VP for Investor Relations along those lines and inquired about the company's views and suggestions for potential legislation. Unfortunately, but not surprisingly, I never received a reply.

[761] see Anna-Marie Wilamovska, et al. *Study on the requirements and options for RFID applications in healthcare*, RAND Europe (2008), Prepared for the Directorate General Information Society and Media of the European Commission, pp. 54-56.

[762] SEC(2007)312, Results of the online consultation on future RFID technology policy.

argue that additional laws could dampen the innovation of new technologies. But, of course this depends on the specific content of those laws.

With the use of RFID and GPS to potentially track and record the movements of people and the consequential threats to privacy in public, the moment is now more than ever to address privacy out in public. As Ramesh (1997) declares, with regards to HIMs, "[t]he time to prevent grievous intrusion into personal privacy by enacting appropriate legislative safeguards is now, rather when it is too late".[763]

Embedding physical objects with RFID tags and the growth of IoT also requires specific legislation, but RFID applications involving individuals, in particular, requires special attention. While state level legislation that addresses RFID/GPS implants and human tracking is a good start, Federal legislation is ideal. Federal laws regulating HIMs and government access to location information would prevent differing state laws. Moreover, the privacy and civil liberty concerns pertaining to HIMs and location information are naturally inter-state issues as people travel across state lines. In any case, as Garfinkel et al. (2005) similarly propose, the law must apply the core principles of privacy protection to RFID systems, which is equally true for both RFID and GPS implants.

7.10.1 Consent

First and foremost, based on the principle of consent, and the general understanding concerning the autonomy of individuals, a Federal law, more comprehensive than the state laws of Wisconsin, North Dakota and California, must explicitly prohibit any private or public entity from mandating or requiring an individual to have a HIM implanted or any other foreseeable tracking or identification mechanism instilled for whatever reason, albeit with certain exceptions. Although consent implies that an individual equally has the right to withdraw his or her consent, the law must also specifically guarantee the right to request the HIM to be temporarily deactivated (if possible) or permanently removed.

The implantation of HIMs should not only at be voluntary (with certain exceptions), but should also never be a condition of exercising another right, including, but not limited to, the right to receive welfare or social security benefits, to work, to vote, to open a bank account, to conduct a commercial transaction, to travel, to take out insurance, to receive medical treatment or to be granted physical access to public or semi-public spaces and, with certain exceptions (see below), government-managed buildings. Hospitals must be prohibited from requiring newly born children to be im-

[763] see Ramesh, Elaine M. *Time Enough? Consequences of Human Microchip Implantation*, Franklin Pierce Law Center (1997), available at: http://www.fplc.edu/risk/vol8/fall/ramesh.htm

planted. Moreover, any individual who consents to be implanted with a HIM, or any other identification or tracking device, must be at least 18 years of age, as Katherine Albrecht equally advocates.[764] But, parents (or legal guardians) may give their consent for their minor children to be implanted.

No individual should be discriminated against by any entity simply because they refuse to have a HIM implanted (or to be tracked by any other device for that matter) nor favored in any way simply because they consented to have a HIM implanted, as advocated by Katherine Albrecht, the Director of CASPIAN, a consumer privacy organization, in her legislative proposals concerning HIMs.[765] Equally, as Spivey (2005) asserts, insurance companies should be prohibited from offering incentives, such as a price reduction or other advantages, in return for their consent to be implanted with a HIM.[766] Any other incentive, discount, or other program that favors implantees must also be prohibited. On the other hand, individuals should equally not be discriminated against for consenting to have a HIM implanted.

Consent, however, may not always be appropriate or required, and may even be at times contrary to the public good and needs of society. Extremely narrow exceptions may apply to convicted violent criminals and the worst sex offenders, where relevant in the vital interest of public security. These individuals could potentially be compelled by the Government to be implanted with a HIM as a condition of parole, subject to Eighth Amendment considerations regarding the prohibition of cruel and inhuman punishment and due process considerations embodied under the Fourteenth Amendment. While Herbert (2006) argues that the Thirteenth Amendment of the US Constitution, which prohibits slavery or forced servitude, could also serve as a basis for prohibiting any mandatory implantation, by comparing mandatory implantation to slavery, there is indeed an exception for the punishment of a crime. Nonetheless, only courts should decide, in accordance with the law, which violent criminal should be compelled to be implanted with a HIM, and not the police nor any other law enforcement agency. Moreover, the basis of the decision should be strictly based on individualized assessments of danger, as opposed to simply mandating, for example, that all sex offenders be implanted, in order to completely avoid legal challenges, as Hinson (2008) argues with

---

764 see Katherine Albrecht's Bodily Integrity Act, available at: http://www.antichips.com/anti-chipping-bill-v07-numbered.pdf

765 see Katherine Albrecht's Bodily Integrity Act, available at: http://www.antichips.com/anti-chipping-bill-v07-numbered.pdf

766 see Spivey, Crystal. *Breathing New Life Into HIPAA's UHID – Is The FDA's Green Light To The VeriChip™ The Prince Charming Sleeping Beauty Has Been Waiting For?* (9 DePaul Journal of Health Care Law, 2005-06), pp. 1317-1342, at 1340.

regards to GPS bracelets. Once the conditions of parole are fully satisfied, the RFID or GPS implant in a convicted violent criminal or sex offender may be removed, if requested by the qualified parolee and equally approved by a court of law.

In addition, certain government employees, which require the highest-level of security, may perhaps reasonably be compelled to be implanted with a HIM as a condition of employment. However, they too must have the right to request the immediate removal of the HIM, if they have resigned or their employment contract has terminated or they have been dismissed. On the other hand, in no circumstances whatsoever, may private entities compel an individual to be implanted.

Any application that removes or diminishes an individual's anonymity with regards to RFID technology must also be prohibited,[767] unless the person concerned gives his or her express consent. Accordingly, the law must prohibit the coupling of the unique ID number of a HIM or any other RFID microchip to information associated with credit or debit cards and any personal information, including name, address, date of birth, telephone number and social security number, unless the person concerned expressly consents otherwise. Equally, the type of information associated with an RFID implant should be at the discretion of the implantee concerned, but narrow exceptions may apply to certain convicted violent criminals and sex offenders.

A person's consent to collect location information through their HIM may also entail the permission to store it for a certain period of time, since that occurs automatically. However, granting permission to collect and temporarily store location information does not entail the permission to disclose it to third parties, without additional explicit permission/consent to do so. The opt-in standard of consent alone must be mandated for the processing or disclosing of location information, lawfully collected and retained through HIMs, or any other RFID tag and/or PLD and/or location-aware device, on each separate occasion. Opt-in consent will endow implantees an opportunity to decide whether or not to allow their location information to be disclosed, essentially returning, for the most part, their ability to control what others may know about them. The opt-in standard of consent in the US is customary. As the FCC points out, most privacy laws in the US "do not employ an opt-out approach but rather require an individual's explicit consent before private information is disclosed or employed for secondary purposes".[768] HIM service providers, data controllers and any other provider of personal tracking or LBS must maintain a record of the opt-in consent and the details of any disclosure of location information, including the name of the third party and the specific purpose of the disclosure. The opt-

[767] see FTC staff report on RFID, p. 20.

[768] Report and Order and Further Notice of Proposed Rulemaking, FCC 07-22, 13 March 2007, p. 26.

in consent must also be explicit and should be invalid if the data subject is not genuinely informed of the purpose(s) of the disclosure (see section 7.10.7).

Similar to the exceptions found in the ECPA, exceptions to the opt-in consent rule, with regards to the disclosing or processing of an implantee's location information, may include the reasonable belief that the disclosure is necessary for emergency response purposes, the fact that the person concerned is knowingly missing or has been kidnapped, the need to execute contractual obligations or the need to comply with lawful requests from law enforcement agencies in possession of a warrant.

7.10.2 Proportionality

The non-consensual based implantation of HIMs must only be permitted if the reasons for doing so are legitimate and proportionate in a democratic and free society. If a less intrusive alternative to HIMs is available, which accomplishes similar objectives and provides similar security benefits, then perhaps that alternative should be used instead. But, as explained earlier, a true alternative to HIMs is not really available at the moment.

Moreover, the quantity and scope of the location information collected and any other personal data associated with HIMs, or any other PLD or location-aware device for that matter, should be in line with the objectives and purposes for which the data was collected in the first place, as specified, for example, in a HIM purpose declaration attached to a standard or tailor-made service provider agreement. No more data than is required to fulfill the specified purposes should be collected and/or linked to the HIM, in accordance with both the *principle of proportionality* and the *principle of data minimization*.

7.10.3 Purpose specification

Those individuals who have consented to have a HIM implanted or have been lawfully compelled to do so, do not simply forfeit their right to privacy and should nonetheless enjoy certain privacy protections and legal safeguards.

The law must prohibit any entity from accessing or monitoring the location information of a person implanted with a HIM, or in any way in possession of a locating/tracking device or embedded RFID tag (i.e. the data subject), outside the designated area and/or scope and specified purpose the same individual has given his/her opt-in consent to have his/her movements to be tracked, such as a secure area or office space, regardless if he/she is traveling in public and especially when he/she is off-duty. Certain exceptions may apply to law enforcement agencies with a proper warrant.

A HIM purpose declaration/end-user agreement/service contract can serve as the legal, as opposed to technological, means of providing not just the opt-in consent, but the basis for any private legal action against a data controller who intentionally collects, monitors or accesses the location information of an implantee beyond the specified and legitimate purposes agreed upon. The purpose declaration can be included in a standard service provider agreement/service contract, binding all relevant data controllers, service providers and any other applicable party, taking into account the relevant laws/regulations. With regards to RFID implantees, the purpose declaration, as the EC similarly recommends for other RFID applications, should specify which data is collected, which association, if any, from the RFID tag to personal data is made, and what the possible privacy risks are.[769]

However, as the EU's Article 29 Working Party points out, "the principle of purpose limitation may be more difficult to apply and to control",[770] without solving the drawbacks of RFID interoperability and ensuring that only authorized readers can read RFID tags.[771] Moreover, if RFID implants are to serve as means of identification for private individuals, then the implants should only respond to trusted RFID readers, in conformity with the "Law of Directed Identity".[772] Where necessary, human-centric RFID systems should provide for mutual authentication, whereby only authorized readers can read the RFID microchips.[773] As proposed by the Article 29 Working Party, one way is to limit the initial query of readers to target only relevant RFID tags in the first place, thereby realizing the collection limitation principle at the protocol level.[774] Similarly, Floerkemeier et al. (2005) proposed that the fair information principles (FIPs) can be incorporated at the "reader-to-tag protocol level", whereby they are implemented

769 see Commission Staff Working Document, Impact Assessment, Accompanying document to the Commission Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification "RFID Privacy, Data Protection and Security Recommendation" {C(2009) 3200 final}.

770 see Working document on data protection issues related to RFID technology, WP 105, 19 January 2005.

771 *Ibid.*

772 The Law of Directed Identity is law number four of the seven Laws of Identity, which were formulated by Kim Cameron, together with other experts online, in order to improve trust in the security and privacy of Internet use. The Laws of Identity are available at: http://www.identityblog.com

773 see Article 29 Working Party, Working document on data protection issues related to RFID technology, WP 105, 19 January, 2005.

774 *Ibid.*, p. 6.

directly at the point of data collection, rather than afterwards,[775] similar to how W3C's Platform for Privacy Preferences Project (P3P) integrated machine readable privacy policies into the browser-to-server protocol, allowing for a user's web browser to automatically read the privacy policy of a website, compare it with the user's preferences, and automatically take action on behalf of the user by either permitting or blocking the transfer of his/her personal data.[776] The incorporation of the FIPs directly into the underlying protocol could also better enable both consumers (data subjects) and data controllers to enforce the corresponding regulations.[777]

In the case of RFID implantees, they could potentially set their privacy preferences, whereby only RFID readers that match these preferences would be allowed to read the RFID implant. As the managers of the RFID Ecosystem[778] proposed with regards to non-implantable RFID tags, RFID implantees could similarly specify rules that describe which TREs should be accessible to which users and which TREs should be deleted automatically (see Rastogi et al., 2007). But, as the managers of the project also point out, this could limit the utility of the system (Ibid.). Juels and Brainard (2004) had earlier suggested a similar idea, which they termed "soft blocking", whereby the data subjects also set their privacy preferences and the RFID readers are designed to comply accordingly. Alternatively, Ayoade et al. (2007) proposed a system called an Authentication Processing Framework (APF) that can potentially authenticate readers before they can access the RFID tag's information in a specific system. The idea is that RFID tags and readers are registered on a database, which then authenticates the readers before being allowed to read the information contained on the registered RFID tags.

The Internet Engineering Task Force (IETF) (see Schulzrinne, H. et al., 2009) has also proposed a protocol-independent model for access to location information. The model includes a Location Generator (LG) that determines location information, a Location Server (LS) that authorizes access to location information, a Location Recipient (LR) that requests and receives location information, and a Rule Maker (RM) that

---

775 see Floerkemeier, Christian., et al. *Scanning with a Purpose – Supporting the Fair Information Principles in RFID Protocols*, Distributed Systems Group, Swiss Federal Institute of Technology (2005), p. 1, available at: http://www.vs.inf.ethz.ch/res/papers/floerkem2004-rfidprivacy.pdf

776 *Ibid.* p. 2.

777 *Ibid.*

778 The RFID Ecosystem is a building-wide RFID project at the University of Washington using thousands of tags and hundreds of readers. The purpose of the project is to demonstrate the risks, benefits, and challenges of user-centered RFID systems and to propose technological solutions to minimizing privacy loss. see RFID Ecosystem, available at: http://rfid.cs.washington.edu/index.html

writes authorization policies. An authorization policy is a set of rules that regulates an entity's activities with respect to privacy-sensitive information, in this case location information. The rule set allows the user to restrict the retention and to enforce access restrictions on location information, including prohibiting any dissemination to certain individuals, during particular times or when in a specific location. The model can also enable the user to control how long the LR may retain the location information and further distribute it.[779]

The 'Internet of Persons' may equally be based on a system whereby the Internet is leveraged, but access to the location information of any RFID/GPS implantee is restricted to those who are registered for the service, logged-in with a username and password and have explicit permission from the implantee concerned to access that information. Therefore, although the means of finding and sharing location information may be available via the Internet, the actual ability to share that information is managed by the implantee.

In addition, the technological, as opposed to legal, means of restricting the tracking of an individual's movements beyond the area in which they have given consent to be tracked may also consist of setting up a so-called "digital territory".[780] In this case, a "digital territory" is simultaneously applied to both the physical and virtual space (Beslay and Hakala, 2007). With regards to HIMs, once an implantee moves outside the designated "digital territory", for instance, the 'bridge' that merges the physical space with the virtual space (*Ibid.*) is temporarily severed until the implantee re-enters into the designated "digital territory".

While obfuscation and anonymity are somewhat suitable technical solutions for other LBS or location-aware applications, these approaches may not be completely suitable for HIMs, since the purpose of HIMs is to in fact accurately identify and track the implantee, albeit under certain conditions, in accordance with the proposed laws and as specified within the implantee's service provider agreement and/or HIM purpose declaration. However, the location information should be rendered anonymous once it is no longer required for the specified purposes it was collected and retained in the first place. Nonetheless, anonymity may be useful to hide the location of individuals in certain areas or during certain time periods. Moreover, as the EC recommends as an

---

[779] see Schulzrinne, H. et al., "Geolocation Policy: A Document Format for Expressing Privacy Preferences for Location-Information", The Internet Engineering Task Force, Internet Draft, February 2009, available at: http://www.ietf.org/id/draft-ietf-geopriv-policy-21.txt

[780] For further discussion, see, for example, Beslay, Laurent., and H. Hakala. "Digital Territory: bubbles" in Paul T. Kidd (ed.) *European Visions for the Knowledge Age: A Quest for New Horizons in the Information Society* (Cheshire Henbury, 2007).

option, a RFID tag could use pseudonyms, whereby the tag can respond with different ID numbers, but the authorized back-office of the system is able to match the different ID numbers to the same RFID tag, whereas this would be much more difficult for an unauthorized party.[781]

7.10.4 Use limitation

While RFID implants are associated with data controllers, they do not necessarily require a wireless service provider. GPS implants, on the other hand, require a service provider, as a result of the required use of a cellular network and the desired storage of the location information. As a service to the customer (i.e. the GPS implantee or data subject), the location information generated by GPS implants should be stored for a certain period of time, in case law enforcement agencies, for instance, need to locate the implantee if he/she is either kidnapped or goes missing.

However, any location information generated by both RFID and GPS implants should be deleted or at least rendered anonymous once it is no longer required for the specified purposes (for example, after 7 days) or should only be retained, in its identifiable form, for a period of time proportionate to the purposes for which it was collected, unless otherwise authorized to be retained for a greater period of time by the implantees concerned.

In addition, the location information should only be retained as long as the service provider or data controller requires it in order to provide the particular services that the implantees have authorized. As the Data Privacy and Integrity Advisory Committee of the DHS similarly proposes, in order to avoid 'function creep',[782] the data collected by

---

781 see Commission Staff Working Document, Impact Assessment, Accompanying document to the Commission Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification "RFID Privacy, Data Protection and Security Recommendation" {C(2009) 3200 final}

782 The term "function creep" refers to any additional use of personal data beyond the specified purposes for which the personal data was permitted to be collected in the first place. Function creep occurs when "personal data collected for one specific purpose and in order to fulfill one function, are used for completely different purposes, which are totally unrelated to the ones for which they were initially collected". Tzanou, Maria. *The EU as an Emerging Surveillance Society: The Function Creep Case Study and Challenges to Privacy and Data Protection* (4 Vienna Online Journal on International Constitutional Law, 2010), p. 421. Function creep "constitutes a breach to the purpose limitation principle" (Ibid.)

RFID technology should only be used for the stated objective and kept "for only as long as necessary to meet the original objective for which it was collected".[783]

A number of difficulties may still arise in enforcing a prohibition on reading RFID implants or other RFID tags on a person without the knowledge and/or permission of that person. To serve as an additional deterrent, the law could potentially also mandate that all RFID readers manufactured for sale in the US make a sound audible within several feet from the reader whenever a HIM or other RFID tag is read, in order to better alert individuals that a RFID tag/microchip has been read. It is already common for RFID readers to make a sound when used in access control systems, such as those found at places of business. Such a measure would be similar to the bill introduced by US Congressman Peter King, which aims to require cell phones containing digital cameras to make a sound when a photo is taken using them, in order to inform individuals that a photo has been taken nearby.[784]

The law should also prohibit the use of read-write tags for the manufacture of HIMs and mandate that HIMs remain passive and are manufactured from read-only or WORM tags. In the case of HIMs manufactured from read-only tags, the data stored on the HIMs should be limited to the unique ID number. In the case of HIMs manufactured from WORM tags, the implantee may request additional information, such as date of birth, in addition to the unique ID number, to be stored on the HIM. While there is no real need for the RFID implant to have much more than the unique ID number stored, RFID implantees themselves should alone have the final say. Nevertheless, it is recommended that only the unique ID number be stored on the RFID implant, as any storage of additional personal data would significantly increase the threat to privacy and data security risk.

Furthermore, the law should also regulate the procedure for implanting HIMs. While the law cannot necessarily prohibit someone from implanting a RFID implant by themselves, it can prohibit the business of implanting HIMs at any place other than licensed clinics, including tattoo or piercing parlors. Moreover, there should be an established protocol regulating not just the implantation of HIMs, but also their removal. A standard waiver agreement should also be adopted and used by all the licensed clinics.

---

783 The Use of RFID for Human Identify Verification, Report No. 2006-02, Data Privacy & Integrity Advisory Committee, Adopted 6 December 2006, p. 11, available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf

784 see H.R. 414, entitled "Camera Phone Predator Alert Act", introduced 9 January 2009. The text of this proposal, however, is already outdated since other devices, such as Apple's iPods and iPads, now have integrated cameras. In Japan, camera phones are already required to make a shutter sound when used.

7.10.5 Enforcement, accountability and redress

Any individual who coerces or compels or otherwise requires another individual to be implanted with a HIM, or in any way implants a HIM in a person without that person's consent, should be subject to criminal penalties. Each violation should be considered a felony, rather than a misdemeanor offense, since it is a serious violation of bodily integrity and a form of physical assault.

Anyone implanted with a RFID implant, or in any way in possession of a RFID tag, is still potentially broadcasting their identity to anyone or anything with a RFID reader several centimeters to a couple feet away. The law should, therefore, criminalize the eavesdropping of RFID implants, without that person's explicit consent, unless done so by law enforcement agencies, in accordance with the law. Accordingly, RFID data transmissions concerning individuals should explicitly be deemed a form of electronic communication, thereby causing the ECPA to apply.[785]

Similarly, the monitoring or interception of the signals of a GPS implant (or any other GPD device) without the knowledge and consent of that person, unless done so by law enforcement agents (under certain circumstances), must also be prohibited.

In order to criminalize the unauthorized interception of the radio signals broadcasted from GPS implants, the ECPA needs to be amended to remove the exception concerning tracking devices (Karim, 2004) and/or the broadcasting of location information, in any form or from any (electronic) source, should also be deemed a form of electronic communication.

It is also critical that statutory law explicitly regards GPS tracking (i.e. electronic tracking) as a search and ensures that the protections of the Fourth Amendment apply (Hutchins, 2007).[786] Equally, when law enforcement agents seek to access or monitor the location information stored on the databases of service providers, for example, in order to conduct an investigation/gather criminal intelligence, statutory law should also specify that a warrant is needed, thereby applying the protections of the Fourth Amendment (Hutchins, 2007) and adjusting the Federal Rules of Criminal Procedure.[787] How-

---

785 see Levary, Reuven R., et al. "RFID, Electronic Eavesdropping and the Law" (RFID Journal, 14 February 2005), available at: http://www.rfidjournal.com/article/articleview/1401/1/128/

786 see Hutchins, Renee. *Tied Up in Knotts? GPS Technology and the Fourth Amendment* (UCLA Law Review, Vol. 55, No. 1, 2007), pp. 409-465.

787 see S.1212, titled "Geolocation and Privacy Surveillance (GPS) Act", introduced 15 June 2011 in Senate by Senator Ron Wyden (D-OR), Sec. 2602. The bill failed to become law.

ever, certain exceptions may apply, in line with existing Federal wiretapping laws.[788] Warrants, for example, should not be required if the individual has presumably been kidnapped or has specifically requested assistance.[789] The law must also explicitly clarify, once and for all, that probable cause alone is required to obtain a warrant or court order to track the movements of an individual and/or to gain access to personally-identifiable location information, based on the belief that the concerned person has committed, is committing or will commit a crime.[790] If deemed necessary or helpful at the initial stages, a dedicated and independent oversight committee could supervise the number of such warrants sought after and obtained, while also ensuring the legal requirements are being fulfilled. The statutory laws, however, should not alter existing legislation on the authority of intelligence agencies to conduct electronic surveillance.[791]

With regards to the private sector, the law must also hold HIM service providers and any other provider of personal locating services, or controller/processor of location information, accountable, if they gather and/or disclose an individual's location information to any private third party without the explicit permission of the person concerned and/or in violation of a standard service provider agreement/HIM purpose declaration. The right to private action against the service providers (or private sector data controllers/processors) should, therefore, also be afforded to implantees who have suffered damages as a result of the unlawful collection and/or disclosure or processing activities.

Accordingly, tort law relevant to privacy intrusion must also be re-defined, whereby location information may pertain to one's private affairs and the disclosure of location information may constitute an invasion upon one's seclusion. This will enable an adversely affected individual, whose location information was unlawfully disclosed/processed, to bring private legal action against any violator and to potentially receive compensation. In order to re-define tort law and permit invasions of privacy in public places to be actionable, McClurg (1995) proposes that the tort of seclusion should take into account, among other factors, the "magnitude of the intrusion, including the duration, extent, and the means of intrusion" (McClurg, 1995).

In order to ensure that the service providers/data controllers are not capable of potentially evading US law, the databases and web-servers associated with US-based

---

788 see 18 USC §2511; S.1212, titled "Geolocation and Privacy Surveillance (GPS) Act".

789 S.1212, titled "Geolocation and Privacy Surveillance (GPS) Act", Sec. 2604.

790 see S.854, titled "The Electronic Rights for the 21st Century Act", Sec. 102, introduced in the US Senate by Senator Patrick Leahy in 1999. The bill failed to become law.

791 S.1212, titled "Geolocation and Privacy Surveillance (GPS) Act".

HIM service providers should be prohibited from being placed in locations outside the jurisdiction of the US.

7.10.6 Access and participation

The law must mandate the ability for implantees to request access to all the information lawfully stored in databases associated with their HIM and be able to delete or correct any such information, at least up to the point permitted so by the service provider agreement and HIM purpose declaration, where applicable.

In the case of implantees under the age of 13, in accordance with the Children's Online Privacy Protection Act (COPPA), the parents or guardians must have the right to access all the information associated with their child's HIM.

Implantees should also have the ability to manage and control how their location information is shared and with whom. As the managers of the RFID Ecosystem proposed and later demonstrated, data subjects can use a web interface to control/manage all the location information (and other data) associated with RFID tags.[792] In the case of RFID implants, implantees should also be able to set privacy preferences, as explained previously in section 7.10.3. The sharing of location information associated with GPS implants could equally be managed online using the protocol-independent model proposed by the IETF.[793] A similar system has already been created by Useful Networks and applied to their *sniff* (Social Network Integrated Friend Finder) location-aware application for smartphones.[794]

Another potential technological solution, albeit farfetched, would be to use RFID microchips with an on/off switch for RFID implants, giving greater control to the implantee. The idea is based on the so-called "right to the silence of the chip". However, knowing when the implant is on or off is another matter.[795] Perhaps, an on/off switch

---

792 see Welbourne, E., et al. *Challenges for Pervasive RFID-based Infrastructure*, PERTEC 2007, Workshop on Pervasive RFID/NFC Technology and Applications, 19 March 2007, available at: http://rfid.cs.washington.edu/images/welbourne-pertec-07.pdf

793 Schulzrinne, H. et al., "Geolocation Policy: A Document Format for Expressing Privacy Preferences for Location Information", The Internet Engineering Task Force, Internet Draft, February 2009, available at: http://www.ietf.org/id/draft-ietf-geopriv-policy-21.txt

794 Useful Networks, at: http://www.useful-networks.com/site/products/community/

795 see Paturi, Prasad. "Switching Off Credit Card Fraud" (RFID Journal, 12 September 2005), available at: http://www.rfidjournal.com/article/articleview/1843/1/82/

could equally be used for GPS implants. A more realistic solution, on the other hand, is the RFID Guardian, developed by a group of researchers, coordinated by Melanie Rieback, from Vrije University Amsterdam. The prototype RFID Guardian is battery-powered and performs 2-way RFID communications, acting both like an RFID reader and an RFID tag. The tool could potentially be an implantee's technological means for detecting the nearby presence of RFID readers, jamming an RFID reader's capability of reading their RFID implant and for providing implantees the ability to control access and authentication.[796] Ideally and for practical purposes, the RFID Guardian will need to be small enough in order to be embedded, for example, within smartphones or other mobile computing devices.[797] The development of radio-reflective shields worn over the area of the body where the implant is located, however, is likely an easier non-technological alternative to the RFID Guardian or on/off switch.

7.10.7 Notice and awareness

As the Data Privacy and Integrity Advisory Committee of the DHS proposed, "[i]ndividuals should know how and why RFID technology is being used, including what information is being collected and by whom".[798] RFID readers in public space must be clearly visible and not covertly hidden. Standardized and generic icons or emblems must also be clearly visible in order to indicate that RFID readers are present nearby[799] or inform individuals that they are entering into a "RFID-read zone" similar to the way the presence of CCTV cameras is indicated.[800] The responsibility of ensuring that this notice is clearly present, accurate and appropriate should fall on both the data controllers and the entity, whether public or private, that has permitted the installation of RFID readers in the specific public space. The signs must accurately reveal the identity and contact information of the data controllers. The signs could also briefly explain the limited purpose and extent of the data collection.

796 For more information on the RFID Guardian project/device, see: http://www.rfidguardian.org

797 *Ibid.*

798 The Use of RFID for Human Identify Verification, Report No. 2006-02, Data Privacy & Integrity Advisory Committee, Adopted 6 December 2006, p. 11, at http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf

799 *Ibid.*

800 see Commission Staff Working Document, Impact Assessment, Accompanying document to the Commission Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification "RFID Privacy, Data Protection and Security Recommendation" {C(2009) 3200 final}.

Preferably, a "universal accepted symbol" should be established, as proposed, albeit unsuccessfully, in a New Hampshire bill.[801] A standard gold icon can already be found on passports from around the world indicating that the passport is embedded with a RFID microchip, but this is not suitable for RFID readers in public spaces. The Association for Automatic Identification and Mobility (AIM) has already developed a RFID emblem free for use, but it is nonetheless still the intellectual property of AIM. An ISO RFID emblem is currently in development. Once adopted, the ISO RFID emblem would be suitable for use in the US and could substitute the need for the US to create and adopt its own emblem. The ISO RFID emblem will contain the data controller's name and contact information.[802]

The implantees should, once again, also be informed via the standardized HIM purpose declaration/end-user agreement/service contract on the purposes of the collection and processing of their personal data.

In addition, the concerned implantees should be notified, where possible, of any unauthorized access and/or disclosure of the location information or other personal information associated with their HIM or of any security breach concerning such information.[803] Implantees should also have the option of being notified of any authorized access of their location information and should have the option of receiving recurring notices on who has been authorized to access this information, obviously with exception to legitimate law enforcement activities.

7.10.8 Security

As the DHS Privacy Office Annual Report to Congress (2007-2008) recommended, several concepts and approaches reflected in the OECD Guidelines for the Security of Information Systems and Networks could be adapted to support the implementation of the OECD Privacy Guidelines.

Any RFID system, especially when involving human beings, as opposed to physical objects or animals, should be carefully designed to prevent the risk of various attacks, such as spoofing or cloning, encryption key cracking and eavesdropping or unauthorized

---

801 N.H. H.R. 203 (defining "universally accepted symbol" as "a graphical system designed to provide a standard way to show the presence of an RFID transponder, its frequency, and data structure").

802 Europe, however, is in the process of creating its own RFID emblem.

803 US Senator Patrick Leahy introduced S.1490, titled "The Personal Data Privacy and Security Act of 2009", which provided for a national standard for data breach notification.

interception. As one commenter urged during the FTC workshop on RFID, "[a]uthorization, authentication, and encryption for RFID . . . [should] be developed and applied on a routine basis to ensure trustworthiness of RFID radio communications".[804] Therefore, RFID implants for human use must no longer be based on the ISO11784/85 standard.

Accordingly, the law should mandate that RFID implants incorporate cryptographic functionalities and use symmetric encryption with a minimum key size of 128 bits, which requires the application of the Advanced Encryption Standard (AES) (Feldhofer et al., 2004). A 128-bit encryption key requires over fifty years to crack with the capabilities of modern computers and the data contained on a RFID tag is basically useless if the encryption key cannot be cracked.[805] Alternatively, instead of using key encryption, RFID implants could adopt Verayo's authentication solution called "Physical Unclonable Functions" (PUFs), which is comprised of tiny, low power circuit primitives that exploit the unlimited, unique variations of the electrical behavior of each silicon chip.[806]

Moreover, since HIMs are a component of an information network, the law must equally mandate that the network itself and the databases that store location information and the personal data associated with any type of HIM (or any other PLD) are equally secure.

A public authority (or authorized third party certification body) can certify that manufacturers of HIMs, data controllers and service providers are meeting these standards. A similar option was recommended by the EC for RFID applications.[807] Any relevant party that fails to implement these security measures may then be held liable.

Accordingly, official RFID security guidelines will be helpful. The German Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik or BSI), for example, has already developed Technical Guidelines on how to implement RFID applications/systems in a secure, but functional way, in order to better ensure the privacy of the associated personal data. The BSI recommended that these Technical Guidelines be incorporated into the pan-European PIA Framework for RFID applica-

---

804 FTC staff report on RFID, p. 20.

805 see Williams, Lorraine C. *A Discussion of the Importance of Key Length in Symmetric and Asymmetric Cryptography*, SANS Institute, GIAC practical repository, 2002, p. 3, available at: http://www.giac.org/certified_professionals/practicals/gsec/0848.php

806 see Verayo, available at: http://www.verayo.com/technology.html

807 see Commission Staff Working Document, Impact Assessment, Accompanying document to the Commission Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification, "RFID Privacy, Data Protection and Security Recommendation" {C(2009) 3200 final}, 5.2.3., Option I.c.

tions.[808] The BSI also plans to offer a certification service that certifies the adequate implementation of these Technical Guidelines.

7.10.9 Privacy Impact Assessment

In addition, the US Government should also formally adopt a comprehensive RFID PIA framework[809] that is similar (though not identical) to the European version.[810] The PIA should be compulsory for any RFID application that involves personal data, regardless whether that data is held by public or private entities.[811]

Accordingly, the law should be altered to require PIAs for both public and private entities, and the requirement should additionally also be relevant for all instances where data processing activities may pose threats to the privacy of data subjects.

Like the EU's RFID PIA framework, the US framework should include the requirement to specifically carry out an *ex-ante* assessment/evaluation of the data protection risks and threats to privacy and, based on the assessment, to identify and evaluate measures to counter, mitigate, prevent and/or eliminate these risks and threats.[812] Furthermore, similar to the EU's PIA framework, the US PIA framework could be primarily

[808] The BSI presented this recommendation during the 3rd meeting of the RFID Recommendation Implementation Informal Working Group at the EC. During the meeting, the establishment of the European RFID PIA was discussed. Industry associations, standardization bodies, public authorities and a representative from the Article 29 Working Party were present at the meeting.

[809] In US law, a PIA is described as "an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks" (E-Government Act of 2002, Section 208).

[810] see Privacy and Data Protection Impact Assessment Framework for RFID Applications, 12 January 2011, available at: http://ec.europa.eu/information_society/policy/rfid/documents/infso-2011-00068.pdf

811 As a step further, PIAs should be mandatory before the deployment of any IT system which involves personal data, regardless of the sector (see Cannataci, 2011). Cannataci also argues that this may be possible in the EU by 2015, as part of the EC's wider review of data protection policy options (2011, p. 180).

[812] For further discussion, see Cannataci, Joseph A. *Recent developments in privacy and healthcare: Different paths for RFID in Europe and North America?* (International Journal of RF Technologies, Volume 2, 2010/2011), pp. 173-187.

developed by significant industry players/stakeholders and reviewed and approved by regulators.[813]

However, contrary to the EU's RFID PIA, the US framework should also be applicable to the manufacturers/developers of RFID infrastructures/systems, and not only RFID application service providers. Therefore, a PIA should be carried out in both stages – before a RFID infrastructure/system is developed and deployed, and before a RFID application/service is developed and deployed. Accordingly, PIAs should be required for both IT service providers *and* manufacturers/developers.

7.10.10 Definitions

The definition of location information would need to be formulated in a way to cover not only the extensively more intrusive location information HIMs are capable of generating, but to ensure, as far as possible, technological neutrality for protecting the privacy of the movements of individuals overall. Instead of the limited scope of location information to telephones, cell phones and computers, as understood within the Telecom Act (and perhaps also by Article 2 of the ePrivacy Directive[814]), the definition should read as follows:

> Location information shall either mean the precise physical location of an identifiable individual at any given moment and/or any collection of the daily movements of that individual tracked over any given period of time, <u>using any means</u>, whether in public or private areas, and shall include, but not limited to, geographic coordinates, street addresses, buildings, landmarks and tag read events, where relevant.

Only then will the privacy of location information or 'location privacy' have real meaning and effect in a court of law in the US.

The definition of a tracking device should also be expanded to include not just electronic devices, such as RFID microchips and GPS devices, but any other automatic iden-

---

[813] see Spiekermann, Sarah. "The RFID PIA – developed by industry, agreed by regulators" in David Wright and Paul de Hert (eds.), Privacy Impact Assessment: Engaging Stakeholders in Protecting Privacy (Springer, 2012).

[814] Article 2(c) of the ePrivacy Directive defines location data as "any data processed in an electronic communications network, indicating the geographic position of the terminal equipment of a user of a publicly available electronic communications service".

tification technology, which permits the tracking of the movement of a person or object.[815] Other automatic identification technologies include Somark's ID system, which is based on "a biocompatible ink tattoo with chipless RFID functionality"[816] and QR code (2D barcode) tattoos. This will allow the law to cover all existing, foreseeable and unforeseeable advancements in human tracking, as similarly pointed out by Albrecht.[817] Accordingly, the modified definition of a tracking device should read as follows:

> *A tracking device shall mean <u>any device, mechanism or system</u> which permits the tracking of the movement of an <u>individual and/or object carried by an individual</u>, either by storing and/or transmitting location information and/or transmitting the identity of an individual via any associated number, symbol, mark or other individual identifier.*

Cyberstalking/electronic tracking laws should be amended to eliminate the restriction that cyberstalking occurs only when the perpetrator threatens, harasses or annoys another person by means of a telecommunications device. This will allow for the prohibition of the use of any tracking device, including HIMs, or any other RFID microchip or GPS tracking device, for the unauthorized tracking of another person, unless done so by law enforcement agencies with a proper warrant.

The Identity Theft and Assumption Deterrence Act of 1998 should already clearly cover identity theft via RFID implants and, therefore, the legislation does not necessarily need to be amended to explicitly include the unique ID number of HIMs.

7.10.11 Constitutional and case law considerations

Above and beyond explicitly regulating HIMs and the use of the location information generated by them, US courts must begin to recognize accordingly that there is an increasing overlap between the private sphere and the public sphere and also that the physical world and the virtual world are gradually merging, as a result of the potential for Internet of Things, Internet of Persons and Ambient Intelligence/ubiquitous com-

---

815 see Katherine's Albrecht's AntiChips website, available at: http://www.antichips.com

816 Somark, available at: http://www.somarkinnovations.com

817 see Katherine's Albrecht's AntiChips website, available at: http://www.antichips.com

puting. Only then will the desired rules concerning HIMs, for instance, and the definition and adequate protection of location information turn out to be legally feasible.

The law must first better accommodate for the fact that one's privacy can indeed be violated while out in public. The analysis of the Fourth Amendment by US courts must, therefore, shift the primary focus concerning the reasonable expectation of privacy from simply where the search is conducted to the nature, content and purpose of the collected information itself (Karim, 2004). Moreover, the reasonable expectation of privacy should rather be driven by the common understandings of the level of privacy society expects overall when out in public. Nissenbaum's "alternative account of privacy in terms of "contextual integrity"" (2004, p. 106) is equally relevant and may also be helpful for understanding the scope of privacy out in public and how it relates to public surveillance. In addition, the courts should also focus more on whether the loss of privacy is desirable or undesirable (Gavison, 1980). In any case, the reasonable expectation of privacy out in public should not be held hostage by the scale of the availability, deployment and use of PITs capable of mass public surveillance.

Regardless if individuals carry around a GPS-enabled smartphone, mobile phone or PLD or have an HIM implanted, it is probably fair to say that most people have a reasonable expectation that their movements or constant whereabouts in public should not be tracked or disclosed without their explicit knowledge and consent, unless done so by law enforcement agencies with a warrant backed by probable cause. In fact, the majority of people believe their movements and whereabouts should be afforded the protections of the Fourth Amendment, albeit to a certain extent. For example, as a survey conducted in California previously showed, 72% of respondents supported legal limits on law enforcement access to location information generated by mobile phones.[818]

Ultimately, courts should officially recognize the notion of 'public privacy', which also deserves protection in tort applications (McClurg, 1995). Stalking laws, as McClurg additionally points out, may already constitute the implied recognition of 'public privacy' (*Ibid*.).

Furthermore, given that the location information generated by RFID implants or constantly transmitted by GPS implants or GPS-enabled smartphones can also be self-incriminating, as Ramesh (1997) points out, the Fifth Amendment should be applied to this location information by categorizing its transmission as a 'communicative act'.[819]

---

[818] see King, Jennifer and Chris Jay Hoofnagle. *A Supermajority of Californians Supports Limits on Law Enforcement Access to Cell Phone Location Information* (18 April 2008), p. 8.

[819] see Ramesh, Elaine M. *Time Enough? Consequences of Human Microchip Implantation*, Franklin Pierce Law Center (1997), available at: http://www.fplc.edu/risk/vol8/fall/ramesh.htm.

7.10.12 The international dimension

As a matter of DHS policy, known as the "Mixed Use Policy", any personal information processed in connection with a 'mixed system'[820] by the DHS should be treated as if it were subject to the Privacy Act 1974, regardless of whether the information pertains to a US citizen, LPR, visitor, or alien.[821] Since implantees from foreign countries who travel to the US should enjoy the same privacy protection rights, the "Mixed Use Policy" should equally be applied to HIMs and any associated databases.

7.11 CONCLUDING REMARKS

RFID or GPS implants do not necessarily need to be banned, as there are public security and personal safety gains, commercial advantages and healthcare delivery benefits to them. Besides, a total ban on HIMs would be an extreme measure and would not necessarily stop with HIMs. Banning HIMs could call into question why other similar or related technologies are not equally banned. Moreover, as the use of RFID and GPS technology grows evermore rapidly, people will, more than likely, accept the existence of HIMs and recognize these benefits, especially if the deployment of HIMs is carried out legitimately and proportionally.

While the security and commercial gains of the widespread deployment and greater use of RFID and GPS technology should be welcomed, the US legal framework, in particular, lacks the appropriate laws to ensure that both the associated privacy threats and security risks are tackled accordingly. However, this is not just a policy or legal issue, but also a matter of technology. Tested technological solutions, mandated by law, are also required.

The establishment and implementation of the required legal and technological safeguards should both ensure that the prospective widespread deployment and use of HIMs, and other applications of RFID and GPS technology, does not erode privacy and personal freedom, while also ensuring that the benefits of RFID and GPS technology, whether security, health, social or commercial, are maintained.

---

[820] A mixed system is a system that contains information on both US and non-US citizens.

[821] see DHS Privacy Office memorandum, *Privacy Policy Guidance Memorandum Number 2007-1 ("Mixed Use Policy")*, issued on 19 January 2007.

8 Conclusions of Part II

8.1 THE NEW THREATS TO PRIVACY

Today, when it comes to privacy issues, there is just too much talk about digital services and social networking websites, such as Facebook,[822] and perhaps not enough attention paid to the potential impending reality that both clothes and walls could be rendered obsolete in terms of protecting privacy, thoughts could potentially be read, DNA analysis could become even more extensive and widespread, the deployment of UAVs could be routine for domestic surveillance, every object or person could be identified and tracked, and every activity out in public could be potentially recorded. Already, body scanners have been deployed at airports around the world, location tracking is commonplace and the advanced surveillance capabilities of CCTV cameras are widespread.

The methods and means of privacy invasion and mass surveillance have never been greater, as the threat to privacy, at present, is often directly relative to the existence and deployment of PITs. On top of that, the threat to privacy and liberty, posed by the latest PITs, are radical, unique and new, and are an affront to all domains and spheres of privacy. For instance, never before has technology been able to potentially see through clothes, read people's minds, track every movement or automatically analyze and possibly predict human behavior.

These new threats to privacy are real and here, and are not hypothetical or potential. Body scanners are rapidly being deployed, enhancements to CCTV cameras are increasingly being carried out and the scope and capabilities of RFID and GPS applications is evermore advancing. While HIMs have not yet reached a critical mass, given the circumstances, there is arguably real potential for their significantly greater (or perhaps widespread) deployment to occur within the next 10 years.

The threats to privacy from PITs are not homogenous and the threats can emanate for different reasons and from different causes. For instance, the threats can come from

---

822 Indeed, however, the threats to privacy posed by Facebook (and other social networking websites) should not be overlooked and are increasingly becoming worrisome.

the abuse or misuse of the privacy-intrusive capabilities of technologies (i.e. when users of PITs intentionally or unintentionally violate privacy and/or data protection laws), or simply from the technology itself regardless of how it is used, or from the intended or unintended purposes of the technology. Moreover, not of all the threats can be predicted and these uncertainties are in themselves a threat and equally should not be ignored (Sollie and Düwell, 2009).

The increasing development, deployment and use of body scanners, HIMs, and CCTV microphones and loudspeakers, not to mention the many other PITs in existence or in development, are changing, where applicable, the level of privacy we enjoy over our physical bodies and the nature of our public space. With the advancement of the latest PITs, the risks, threat level and temptation of abuse have drastically increased. The means of privacy invasion and mass surveillance have never been greater and the threats to privacy and liberty posed by the latest PITs are uniquely new.

However, that does not mean that any or all of the PITs addressed should be completely banned. That would require a complex explanation and methodology of determining what technologies should be considered acceptable and unacceptable based on a comprehensive ethical framework on evaluating technology.[823]

On the contrary, these technologies should arguably be embraced, as long as the adequate legal framework is in place. Although PITs pose serious threats to privacy, they offer in return a common good, i.e. potential benefits in terms of security, convenience, electronic commerce and, in the case of RFID implants, also improved and safer healthcare delivery. Nevertheless, while benefits exist, the threats and risks persist.

8.2 BEYOND PRIVACY AND DATA PROTECTION

If left unchecked and without the adequate legal framework in place, the latest PITs threaten not just the right to privacy, but other individual civil liberties as well. The latest PITs pose a threat to other civil liberties by causing a 'chilling' effect on fundamental rights, such as the freedom of speech, freedom of association and freedom of movement – freedoms, which are necessary in a free and democratic modern state. This is particularly true for technologies capable of mass public surveillance.[824] For instance, the intrusive

[823] For further discussion, see Sollie, Paul and Marcus Duwell (eds)., *Evaluating New Technologies: Methodological Problems For The Ethical Assessment Of Technology Developments* (Springer, 2009).

[824] For further discussion, see the Memorandum by Victoria Williams for the House of Lords Constitution Committee inquiry into the impact of surveillance and data collection upon the privacy of citizens, available at: http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/8051402.htm

capabilities of HIMs could have a ‘chilling’ effect on the freedom of movement, as people become more cautious where they travel. HIMs, or the RFID microchips in travel cards for that matter, could also be used to interfere with the freedom of movement by denying or ‘digitally cutting-off’ a person’s access to mass public transportation. The capability of CCTV microphones, if left unchecked, could potentially have a ‘chilling’ effect both on the freedom of expression out in public and the freedom of assembly, and, thus, could also frustrate the right to protest peacefully. CCTV loudspeakers could especially have a detrimental effect on personal autonomy and dignity.

Besides, the right to privacy and data protection laws are not always enough to defend liberty or check every threat posed by the latest PITs. In the US, the freedom from unreasonable search, embodied in the Fourth Amendment of the US Constitution, serves as the basis of the reasonable expectation of privacy. But, this expectation is subjective and vulnerable to the constantly advancing development and deployment of PITs. Moreover, even though location information can potentially reveal sensitive personal information, the location information generated by RFID and GPS applications is not necessarily or adequately afforded the protections of the Fourth Amendment, due to the current ambiguous division of what is private and what is public, and the lack of a legal recognition of privacy out in public.

In the EU and the UK, data protection laws were formulated, for the most part, to control personal data, which is conventionally understood to mean information that relates to identified or identifiable individuals. But, this formulation also certainly has its downsides. For instance, even though the images produced by (fully-intrusive) body scanners are seriously privacy-invasive, the images may not necessarily always constitute personal data or data in personally identifiable form *per se*, since a person arguably cannot be identified from the images alone, and therefore data protection laws alone may not be applicable or sufficient for regulating body scanners. While the recording of general sound out in public by CCTV microphones is intrusive, it is also arguably not considered personal data *per se* and, therefore, is not covered by data protection laws in the UK (since it is not focused on any particular individual, in accordance with UK case law). Data protection laws also do not apply to CCTV loudspeakers, since the loudspeakers are not used to process personal data, but CCTV loudspeakers, nonetheless, may pose a threat to the right to be left alone. Likewise, even when the use of RFID microchips is not initially linked specifically to identified individuals, threats to privacy still remain, since the data could potentially later be used, nonetheless, to identify, track and profile individuals. This brings us to the next downside. Data protection laws do not apply to anonymized data. However, with advanced data mining techniques and group profiling (i.e. the categorization of people), the effects could be just as bad as (or even worse than) processing personal data.[825] Moreover, while the Data Protection Directive (Directive 95/46/EC) is certainly applicable for transactional acts, the Directive may not cover adequately non-transactional acts, such as interactions/relationships and opinions.

Applying the principles of privacy/data protection alone, therefore, cannot entirely address the potential impacts and threats of public surveillance technologies. As Victoria Williams equally reminds us, in order to assess the impact of public surveillance schemes, the consideration of the effects on personal autonomy is required, concluding that lawmakers must also assess how the observation of public places creates a risk of 'chilling' the right to exercise the freedom of speech and assembly.[826] Accordingly, the right to privacy and other civil liberties or human rights need to be protected in an integrated manner. The legal framework should, as a result, not only focus on the right to privacy and data protection, but rather also emphasize on safeguarding other fundamental rights, where applicable, and better extending the regulation of privacy infringement into other domains, such as the human body and the public sphere. Hence, the legal and technical solutions for addressing the intrusive capabilities of PITs must not only be concerned with the right to privacy, but should also take into consideration, where applicable, other civil liberties and social and moral issues simultaneously.

8.3 DEFICIENCIES OF THE EXISTING LEGAL FRAMEWORKS

The legal framework in the US, as it stands now, is unequipped, for the most part, to meaningfully counteract the privacy threats posed by body scanners and HIMs, while the UK legal framework is equally inadequate to regulate CCTV microphones and CCTV loudspeakers. In terms of fulfilling the principles of privacy, with regards to these latest technologies, the deficiencies and dilemmas of the US and UK legal frame-

[825] For that reason, the Article 29 Working Party specifically addresses this issue and argues that the scope of Directive 95/46/EC applies to targeted profiling/online behavioral advertising. see Article 29 Data Protection Working Party, WP 171, Opinion 2/2010 on online behavioural advertising, 22 June 2010.

[826] see *supra* note 824.

works are evident. As deducted from the case studies, the deficiencies of the current legal framework, pertaining to privacy/data protection in the US and the UK/EU, are partly due to the fact that traditional policy or legal-based solutions focus predominantly on data controllers/processors, service providers and operators/users of PITs, as opposed to their developers/manufacturers. This approach fails to address the privacy-intrusiveness of the technologies concerned at the design stage.

While there are certainly significant deficiencies in the US and UK legal frameworks, with regards to the latest PITs, neither legal framework necessarily requires a complete overhaul. Instead, the legal frameworks require both amendments to existing laws, and new laws based on what continues to remain valid.

Moreover, while some might argue that the privacy principles are losing validity, particularly in light of the latest technologies and the impending ubiquitous information society; this is only true if we let this occur. As demonstrated through the case studies, the common principles of privacy protection can still form the foundation to work from, and there is no need to reinvent the wheel at this juncture. The current principles of privacy indeed remain as the basis of assessing the adequacy of a legal framework in terms of protecting privacy and continue to be relevant and valid both for formulating new legislation and designing for privacy. However, this does not mean that there is no need whatsoever now or in the future to revisit the privacy principles, where necessary, or to even establish and add new principles.[827]

Nevertheless, what is most essential is that there are adequate means, mechanisms and methodologies for enforcing and implementing the existing privacy principles against the evermore advancement of technology. Although both the US and UK/EU legal framework express the goals and elements of privacy protection, the practical rules on how to realize them are inadequate. Without adequate and specific rules in practice, the developers of body scanners, HIMs and CCTV microphones and loudspeakers, for example, are left to voluntarily determine their own way of realizing these goals, and thus their level of responsibility for doing so or lack thereof.

Indeed, there is a vacuum of law, which must be dealt with accordingly, in order to bring the law up to speed with the latest threats to privacy and other civil liberties posed by the latest technologies. Throughout this dissertation, the recommendations on dealing with the deficiencies of the US and UK legal frameworks primarily focused on *both* legislative/policy and technological solutions, based on the widely established fundamental principles of privacy, as opposed to overhauling or reversing the problem-

[827] Indeed, the OECD Secretariat supports a "global privacy dialogue" that is intended to revisit the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. see the DHS Privacy Office Annual Report to Congress, July 2007-July 2008, p. 77.

atic, altering (and potentially somewhat outdated) analysis and interpretation of courts within the US and UK.

While there is, to a certain extent, already a legal basis for PBD within the US and UK/EU legal frameworks (see section 9.6), the prevailing deficiency concerns the fact that the relevant provisions are primarily only applicable directly to data controllers and service providers, as opposed to the designers and/or manufacturers of the PITs themselves. Data protection/privacy laws and regulations have all too often focused on requiring data controllers/processors to comply. Unfortunately, even the draft proposal for an EU General Data Protection Regulation,[828] while indeed a step in the right direction, proposes *data protection by design* (i.e. PBD) requirements that are erroneously only applicable to data controllers.[829]

Although the laws could have an indirect effect on manufacturers, whereby the data controllers in turn compel or put pressure on manufacturers, this has evidently proved insufficient. Instead, the law should specifically emphasize additional obligations on the manufacturers/developers.

Part II evaluated/assessed the adequacy of the legal frameworks in the US and the UK and proposed some of the necessary amendments to enhance these legal frameworks, in order to ensure that the right to privacy is preserved, in light of the intrusive capabilities of the four particular PITs addressed. In addition to the proposed legal solutions, a number of technical and/or design solutions were proposed for each PIT. Technical and design solutions for the sake of protecting privacy are collectively known as "privacy by design". The next chapter (Chapter 9) outlines what is specifically meant by "privacy by design".

[828] see Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11/4 draft.

[829] *Ibid.*, Article 23.

PART III

9 Privacy by design

9.1 CHAPTER INTRODUCTION

Privacy by Design (PBD) is a relatively novel concept that is now at the centre of the privacy debate among legal scholars and lawmakers/policy makers.

Section 9.2 outlines the concept, origins and premise of privacy of design. Section 9.3 gives a brief overview of the overall methodology behind privacy by design. Section 9.4 summarizes the privacy by design possibilities for the four case studies. Section 9.5 explains the similarities and differences between privacy by design and privacy-enhancing technologies. Section 9.6 outlines the applicability of privacy by design within the US and EU/UK legal frameworks. Section 9.7 provides an overview of the growing recognition among legal scholars and policy makers of the benefits and necessity of privacy by design. Section 9.8 outlines the potential increase in the use of privacy-enhancing technology/privacy by design. Section 9.9 explains why there is a growing need for privacy by design, due to the increasing lack of trust of citizens/consumers. Section 9.10 explains why privacy by design can potentially be good for business. Section 9.11 outlines some of the criticism of privacy by design. Section 9.12 outlines some of the practical challenges of implementing PBD. Section 9.13 concludes with some ending remarks.

9.2 CONCEPT AND ORIGINS OF PBD

Technology, and its rapid advancement thereof, has increasingly received attention from the field of ethics, which has evolved from being fully occupied on theory to focusing on the sensitivity to values ‘‘built in’’ to technology and the process of doing so (Albrechtslund, 2007, p. 64). Hence, value sensitive design (VSD) or similarly “values in design” (see Flanagan et al., 2008) was born. ‘‘Value Sensitive Design is a theoretically grounded approach to the design of technology that accounts for human values in a principled and comprehensive manner throughout the design process'' (Friedman et al., 2002, p. 1). VSD assumes:

> that human values, norms, moral considerations can be imparted to the things we make and use and it construes information technology (and other technologies for that matter) as a formidable force which can be used to make the world a better place, especially when we take the trouble of reflecting on its ethical aspects in advance (van den Hoven, 2007, p. 67).

In terms of ICT, VSD is not the same as "digital ethics", which "refers to *human* ethical behaviour when using *digital* devices (or, more generally, ICTs)" (emphasis added).[830] Instead, VSD emphasizes the social and ethical responsibility of scientists, inventors, engineers or designers when researching, inventing, engineering and/or designing technologies that have or could have a potentially profound effect (negative or positive) on society. By combining values and norms with the development of technology or 'embedding ethics' into technology (Aarts and de Ruyter, 2009, p. 11), VSD can create what is known as "normative technology". Although VSD was first proposed in connection with ICT, it has wider applications (van den Hoven, 2007, p. 67). For example, VSD may even apply to the manner in which bombs/missiles are designed and developed to better comply with international laws of armed conflict and other human norms.

In *Code and Other Laws of Cyberspace*, Lessig (1999)[831] outlined how regulating technology has four interacting and complimentary modalities, dimensions or mechanisms*: laws; norms; market*; and *physical architecture*, and how the effective regulation of technology can be achieved through the optimal combination of these elements. Computer code, for Lessig, is a form of architecture and, thus, has similar abilities to regulate human behavior (Grimmelmann, 2005). Lessig was essentially one of the first authors to highlight how computer code and the Internet's architecture/protocols can be more effective in regulating online activities and ensuring online privacy than written legal code or a website's privacy policies. For Lessig, computer code could also give users greater control over how their personal data is used, a concept Lessig terms "privacy control" (Schwartz, 2000). Machine-to-machine protocol, for instance, could enable a web browser and website to negotiate, on behalf of the individual web

830 Barbat, Boldur., Andrei Moiceanu, Hermina Anghelescu. "Enabling Humans to Control the Ethical Behaviour of Persuasive Agents" in Eugene Loos, Leslie Haddon and Enid Mante-Meijer (eds.) *The social dynamics of information and communication technology* (Ashgate, 2008), pp. 191-203, at 193-94.

831 An updated version of the book came out in 2006. Lessig, Lawrence. *Code and Other Laws of Cyberspace, Version 2.0* (Basic Books, 2006).

user, based on the personalized privacy preferences set by the user.[832] W3C's Platform for Privacy Preferences Project (P3P) is significantly based on this concept (Schwartz, 2000). As a result of Lessig's work, the use of computer code to implement legal code and regulate or restrict human conduct/behavior is now widely known as "code as law" (or "law as code").[833]

Reidenberg (1998, 2000), for instance, similarly argues that data protection/privacy is collectively derived from politics, economics and technologies, whereby the political model employs laws, the economic model employs market norms/self-regulations and the *Lex informatica* model applies the use of technologies/technical protocols.[834] Reidenberg (2000) equally points out that "the most direct regulation of information processing comes from the technological rules built into network infrastructures by industry rather than from law itself" and "these technical rules define the capabilities of networks such as the Internet to invade or protect privacy".[835]

Gaining insight from Lessig, other legal scholars have further built on the concept of "code as law" and have likewise voiced their belief in the important role computer code, design-based solutions and 'normative technology' can play in regulating technologies (see, e.g., Tien, 2004; Leenes and Koops, 2005; Grimmelmann, 2005; Brownsword, 2005; Hildebrandt, 2009; Hildebrandt and Koops, 2010; Yeung and Dixon-Woods, 2010).

Grimmelmann (2005) critiques, for various reasons, Lessig's assumption that code is a form of architecture, while acknowledging the very effective role software/computer code can play in regulating human behavior and the importance of different modalities of regulation. Instead, Grimmelmann argues that "computer software is its own distinctive modality of regulation, and it needs to be treated as such" (2005, p. 1722).

---

[832] see Lessig, Lawrence. *Code and Other Laws of Cyberspace* (Basic Books, 1999), p. 160. For further discussion, see Schwartz, Paul M. *Beyond Lessig's code for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices* (Wisconsin Law Review, Volume 2000, Issue No. 4, 2000), pp. 743-787.

[833] see Lessig, Lawrence. *Code and Other Laws of Cyberspace* (Basic Books, 1999).

[834] Reidenberg Joel. *Lex Informatica: The Formulation of Information Policy Rules Through Technology* (Texas Law Review, Volume 76, No. 3, 1998), pp 553-93.; Reidenberg, Joel R. *Privacy Protection and the Interdependence of Law, Technology and Self-Regulation* (2000), available at: http://reidenberg.home.sprynet.com/Interdependence.htm

[835] *Ibid*.

For Grimmelmann, three basic characteristics of software make it different: software is *automated*;[836] software is *immediate;*[837] and software is *plastic*.[838]

Privacy by design[839] (PBD) is essentially *both* a form of VSD and "code as law". Similarly, PBD is the realization of values, in this case the principles of privacy and corresponding rules/regulations, via the physical design, technical specifications, architecture and/or computer code of the device, system, technology or service concerned, where applicable. The aim of PBD is to design and develop a system or device (i.e. software and/or hardware) in a way that supports and materializes those principles, values and rules as goals and functions, whereby that system or device then becomes 'privacy-aware' or 'privacy-friendly'. Through PBD, which Hildebrandt and Koops (2010) term "ambient law" when applied to "ambient intelligence", the legal protections and legal norms are essentially articulated within the technical infrastructure and there is a movement from simply legal protection to *legal protection by design* (see Hildebrandt and Koops, 2010). In other words, PBD can be defined as practical measures, in the form of technological and design-based solutions, aimed at bolstering privacy/data protection laws, better ensuring or almost guaranteeing compliance, and minimizing the privacy-intrusive capabilities of the technologies concerned. Thus, PBD is part of the emergence of a new paradigm to protecting privacy, "in which system designers conduct privacy risk assessments and incorporate privacy as a fundamental design parameter" (Duncan, 2007). However, PBD is more than ethical design (or VSD), since it is also based on law and must be both technological and legal at the same time (Hildebrandt and Koops, 2010).

Perhaps, further building on Lessig's notion, Gaurda and Zannone (2009) also articulated PBD as an approach to bridging the difficult gap between legal (natural) language and computer/machine language to develop "privacy-aware systems".[840] This

[836] "Once set in motion by a programmer, a computer program makes its determinations mechanically, without further human intervention" (Grimmelmann, p. 1723).

[837] "Rather than relying on sanctions imposed after the fact to enforce its rules, it simply prevents the forbidden behavior from occurring" (Grimmelmann, p. 1723).

[838] "Programmers can implement almost any system they can imagine and describe precisely" (Grimmelmann, p. 1723).

[839] Ann Cavoukian, Ontario's Informational and Privacy Commissioner, first coined the term "privacy by design" during the 1990s. see Cavoukian, Ann. *Privacy by Design* (2009). Cavoukian has been a key outspoken supporter of the widespread adoption of PBD, and now also refers to PBD (i.e. the designing of technology to be privacy-friendly) as "smart privacy".

[840] Guarda, Paolo., and Nicola Zannone. *Towards the development of privacy-aware systems* (Information and Software Technology, Volume 51, Issue 2, February 2009), pp. 337-350.

branch of PBD especially focuses on the use of software or computer code as a means of enforcing privacy rules and regulations. One of the goals of PBD, therefore, could be to create devices or systems that are capable of effectively implementing laws and rules that we as humans understand in the form of legal natural language (LNL) and devices, systems, computers, etc. understand in the form of legal machine language (LML).[841] This approach has been proposed/developed for enhancing the "safety intelligence" of Next Generation Robots (NGRs)[842] and may also be applicable for better ensuring the privacy friendliness/privacy awareness of other technologies.

The premise behind PBD is that it is likely more effective to enforce laws/rules at the manufacturer/design-level, as opposed to the user-level, by engineering into the relevant system or device the (legal) requirements, where applicable. This is known as "legal requirements engineering" (Schmidt and Franken, 2003). In the case of privacy, "legal requirements engineering" can be more specifically termed "privacy engineering", which is essentially just another name for PBD. Kenny and Borking (2002) defined "privacy engineering" "as a systematic effort to embed privacy relevant legal primitives into technical and governance design".[843]

As opposed to being centered on technology users and data controllers, PBD is ideally centered on technology developers/providers and manufacturers. The focus of privacy law and the burden of compliance, responsibility or liability are, therefore, shifted to the designers/engineers and manufacturers/developers of the technologies (software or hardware) concerned and further away from the operators or controllers of these technologies and/or the application service providers. While there is still a need for controllers and service providers to also implement PBD, there is, nonetheless, a shift in focus brought about by PBD, placing manufacturers/developers at the center of implementing privacy/data protection laws.

Although the focus of this dissertation is primarily on the manufacturers of hardware (i.e. body scanners, RFID microchips, CCTV systems), PBD is certainly also applicable to digital services/products/technologies,[844] since the use of computer code

841 see Yueh-Hsuan Weng, Chien-Hsun Chen and Cheun-Tsai Sun. "Safety Intelligence and Legal Machine Language-Do we need the Three Laws of Robotics?", in Yoshihiko Takahashi (ed.) *Service Robot Applications* (InTech Education & Publishing, August 2008), available at: http://works.bepress.com/weng_yueh_hsuan/3

842 *Ibid.*

843 Kenny, Steve. and John Borking. *The value of privacy engineering* (Journal of Information, Law and Technology 2, 2002), available at: http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2002_1/kenny/

844 Digital services include, for example: online social media/networking services (e.g. Facebook, Twitter, LinkedIn, etc.); cloud computing (e.g. Google Docs); e-mail (e.g. Gmail, Hotmail, etc.); and web advertising services/tools.

is one tool in the PBD toolbox. In fact, a recent FTC Staff Report, titled "Protecting Consumer Privacy in an Era of Rapid Change", which contains a somewhat extensive discussion on PBD, focuses primarily on applying PBD to digital services.[845] Indeed, digital services/products certainly may pose some of the most serious threats to privacy at present, but when it comes to PITs this is just the tip of the iceberg.

However, it is also important to emphasize here that PBD does not only necessarily pertain to technical specifications, technological solutions or computer code, but also to the actual physical design or architecture of the device or system concerned. Take for example an automated teller machine (ATM). As Little et al. (2005) distinctively point out, the physical design (i.e. the height of ATMs, surrounding barriers, and size of the computer screens) equally affect the privacy of the user's personal identification number (PIN) and information displayed on the screen, and ability thereof to cover up this information, as much as the technical security specifications of the ATM's internal system itself.[846] In a similar sense, PBD also applies to voting booths or enclosures, which require a certain (physical) design in order to better ensure the sanctity of one's vote.

When PBD does pertain to a technological solution, the solution also does not necessarily need to be so sophisticated. PBD solutions range in degree of sophistication, from advanced privacy algorithms for the images generated by public surveillance cameras or body scanners to simple snapshot sound effects for digital cameras or the use of only optional data fields in the design of information systems as far as possible (Borking, 2010).

It is also important to stress that the goal of PBD is not to manage the evolution of technology. Therefore, PBD should theoretically not be viewed as hostile to innovation. Instead, PBD simply seeks to ensure that privacy is taken into consideration or built-in at the earliest stage of the device or system's lifecycle, i.e. when the device or system is being designed and manufactured, as opposed to 'glued on' or 'bolted on' after the device or system has already been developed (Cavoukian, 2009). In essence, PBD is meant to serve not as a barrier to technology, but rather as a guided driver of technological development.

---

[845] As a follow-up to the preliminary FTC Staff Report, the FTC Final Report, "Protecting Consumer Privacy in an Era of Rapid Change", was published in March 2012, available at: http://ftc.gov/os/2012/03/120326privacyreport.pdf

[846] see Little, Linda., Pam Briggs and Lynne Coventry. *Public space systems: Designing for privacy?* (International Journal of Human-Computer Studies, Volume 63, Issues 1-2, July 2005), pp. 254-268.

Nevertheless, PBD should be considered as a full lifecycle approach (i.e. at every stage in the product's development, starting from conceptualization).[847] As the Privacy By Design Report from the UK's ICO equally points out:

> For a privacy by design approach to be effective, it must take into account the full lifecycle of any system or process, from the earliest stages of the system business case, through requirements gathering and design, to delivery, testing, operations, and out to the final decommissioning of the system. This lifetime approach ensures that privacy controls are stronger, simpler and therefore cheaper to implement, harder to by-pass, and fully embedded in the system as part of its core functionality.[848]

PBD is part of a paradigm shift to enforcing privacy laws and addressing privacy concerns through design practices. The shift began with 'code as law', but has now evolved to a more holistic approach for fully regulating the technical specifications/architecture of a device/system for the sake of safeguarding privacy. Above all, PBD can be considered a product of a growing movement, whereby design is positioned front and center for solving problems, as promoted by Berger (2009), and a growing emphasis on designing hardware and software in the context of social practices and human needs, as advocated by the European Society of Socially Embedded Technologies (EUSSET).[849]

Thus, here design is not about aesthetics, but about utility. For example, there is also a design practice known as 'design for all', whereby objects, devices, buildings, etc. are designed to be accessible and useful for as many people as possible, including the elderly and disabled.[850] 'Green by design' is another design practice, whereby objects, buildings, etc. are designed to have the lowest 'carbon footprint'. The same goes for reducing the greenhouse gases emitted from automobiles and the energy consumption of buildings, where the design and development stages may often critically define the environmental impacts of the final products. Based on the same premise why 'green

---

[847] see the FTC Final Report, "Protecting Consumer Privacy in an Era of Rapid Change", March 2012, available at: http://ftc.gov/os/2012/03/120326privacyreport.pdf

[848] Privacy By Design Report, Information Commissioner's Office, 2008, p. 7, available at: http://www.ico.gov.uk/upload/documents/pdb_report_html/privacy_by_design_report_v2.pdf

[849] see EUSSET's position paper, available at: http://www.eusset.eu/uploads/media/MANIFESTO.pdf

[850] Similar to PBD, 'design for all' does not necessarily require high-tech technological solutions, and can range from simply large dialing buttons on a telephone to highly advanced brain-to-computer interfaces (BCI).

by design' is now considered necessary to save the planet, and 'design for all' is considered necessary to meet the needs of the elderly or those with disabilities, 'privacy by design' may also be necessary to safeguard privacy in the 21st Century.

PBD can also be viewed as part of the growing recognition in the need for ethically and legally sound research and technological development (RTD), in line with human rights laws, and the consideration of the societal issues concerning RTD. PBD, in this sense, can be a way of governing RTD, ensuring that RTD is in line with the principles of privacy and ethics, and can serve as a means of balancing the societal demands for the preservation of privacy and the societal needs and goals of RTD.

An analogy of PBD is the engineering of the requirements of traffic, environmental and fuel efficiency laws within automobiles. Some vehicles even have built-in limitations on their maximum speed capability, which is obviously more effective in enforcing the speed limit, than mandating that drivers do not exceed a 120-140 kilometer-per-hour (kmph) speed limit in cars that can reach speeds up to 260 kmph or more. As the Royal Academy of Engineering similarly points out, "[j]ust as security features have been incorporated into car design, privacy protecting features should be incorporated into the design of products and services that rely on divulging personal information".[851]

9.3 PBD METHODOLOGY

The execution of PBD is not fixed and there are a variety of different approaches. Essentially, "there is no well established and worldwide accepted view on the way privacy protection and the consolidation thereof can be built into software" (van Blarkom, G.W. et al., 2003, p. 2). The same is true for PBD overall.

On this note, the consortium for the Privacy Incorporated Software Agents (PISA) project, funded under the European Framework Programme, set out to establish an accepted methodology for incorporating privacy protection into software and to address the technical challenges of data protection. The project developed Privacy Enhancing Technologies (PETs), which can protect the privacy of individuals when they use services provided through software agents.[852] In doing so, the PISA project also formulated a process that included analyzing the legal requirements to determine the

---

[851] Dilemmas of Privacy and Surveillance: Challenges of Technological Change (The Royal Academy of Engineering, London, 2007), p. 7, available at: http://www.raeng.org.uk/news/publications/list/reports/dilemmas_of_privacy_and_surveillance_report.pdf

[852] see van Blarkom, G.W., J.J. Borking, J.G.E. Olk (eds.). T*he Handbook of Privacy and Privacy-Enhancing Technologies: The Case of Intelligent Software Agents* (2003).

required human behavior, then translating privacy laws and data protection rules into design or technical solutions for each requirement, based on the "engineering psychology" approach, and subsequently conducting a privacy audit.[853] It is, however, also first necessary to investigate the privacy threats or risks posed by the technology concerned.

While the *Handbook of Privacy and Privacy-Enhancing Technologies* (van Blarkom, G.W. et al., 2003), created by the PISA project consortium, provides a methodology for designing for privacy, it is more relevant for developing PETs and middleware to protect privacy, than for PBD. The methodology, called "Design Embedded Privacy Risk Management" (DEPREM), was developed to realize "privacy knowledge engineering" (PYKE), in order to build the privacy principles and data protection rules, based on the formulation of ontologies,[854] into an intelligent software agent (*Ibid*., p. 169). Ontologies can help to provide the common language and understanding necessary for incorporating the principles of privacy into the design and architecture of technologies (van Blarkom, G.W. et al., 2003) and, therefore, for interpreting legal code into technical/computer code, thereby also potentially helping to bridge the difficult gap between natural language and computer language (see Gaurda and Zannone, 2009).

The methodology formulated by the PISA consortium may be certainly helpful for formulating an overall process of designing for privacy that is repeatable. Essentially, the overall objective and approach of PBD is to go from written privacy/data protection laws, regulations, privacy principles, norms and civil liberties that regulate human behavior and grant individuals certain rights/freedoms to the realization of technological/design solutions that minimize the intrusive capabilities of a device, product or service and implement those laws and principles (see Figure 3).

---

[853] see Patrick, A.S., and Kenny, S. *From Privacy Legislation to Interface Design: Implementing Information Privacy in Human-Computer Interfaces*. Paper presented at the Privacy Enhancing Technologies Workshop (PET2003), Dresden, Germany, 26-28 March, 2003, p. 2.

[854] Ontologies are formal machine understandable descriptions of terms or concepts and the relationships between those terms or concepts in a particular domain (van Blarkom, G.W. et al., 2003, p. 169).

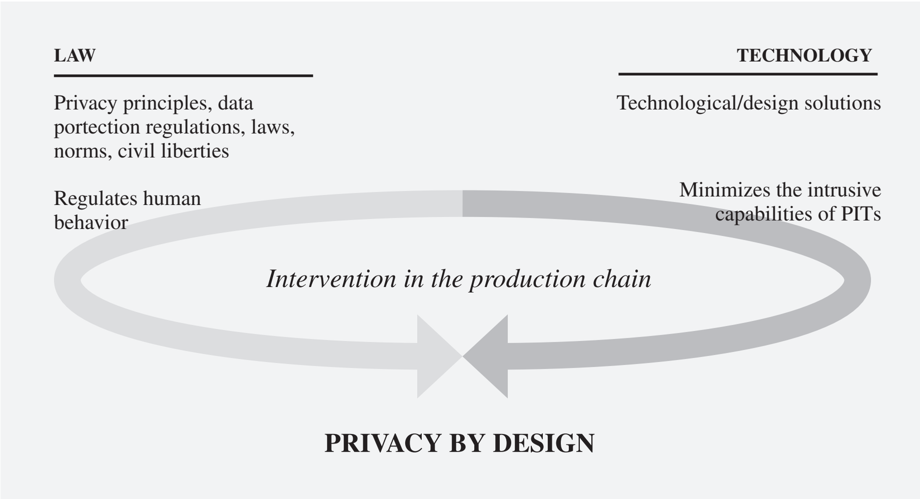

Figure 3: PBD overview

It is important to note, once again however, that the design and technical requirements must be directed at the designers, engineers, developers and manufacturers of PITs and not, or at least not solely, at the data controllers and/or operators and/or processors and/or application service providers. This is a policy mistake the PISA consortium promoted, contrary to the value and purpose of PBD, which requires intervention before the main technical and design specifications of the product, device or service are set in stone.

On the other hand, the PISA consortium should not necessarily be blamed, as they were merely applying the law, since Directive 95/46/EC is only applicable to data protection controllers and processors. However, solely directing technical requirements to data controllers/processors may overestimate their technical abilities and resources. As the Article 29 Working Party points out, data controllers can hardly be considered in a position to take any relevant data/privacy protection measures by themselves even if they wanted to.[855] This approach may also underestimate the difficulty and inefficiency of incorporating privacy protection solutions after the devices/systems have already been developed and deployed.

[855] see Article 29 Working Party, The Future of Privacy, 1 December 2009, WP 168.

9.4 PBD SOLUTIONS: BODY SCANNERS, HIMS, CCTV MICROPHONES, LOUDSPEAKERS

While practical challenges exist, the numerous proposals for safeguarding privacy, in light of the deployment and use of body scanners, HIMs, and CCTV microphones and loudspeakers, as earlier explained and recommended, include credible and feasible technical/PBD solutions mandated by law. For those who believe that PBD is a great idea in theory, but question its effectiveness in practice, need only to consider some of the technical or PBD solutions proposed and outlined in Chapters 5, 6 and 7 of this dissertation and those already being developed, tested and deployed.

PBD solutions for body scanners include the built-in use of privacy filters or privacy algorithms for body scanners, the remote separation of the console where the images are viewed from where the passengers are scanned, encryption and secure cable connections. The use of 'intelligent detection software' to discern dangerous objects, instead of using human screeners, is also a potentially viable PBD solution, but may still require further development and testing.

PBD solutions for HIMs include, for example, embedded encryption and protocol-level controls in RFID implants, and secure web interfaces to enable implantees or other end-users of location-aware devices, PLDs and LBS to access and participate in the generation, storage and availability of their location information.

PBD solutions for CCTV microphones include, for example, the use of artificial intelligence/software agents to permanently limit the activation of the recording capabilities of the microphones only when certain sounds considered dangerous or threatening are detected. PBD solutions for CCTV loudspeakers include the use of pre-recorded messages to permanently limit what can be communicated through the loudspeakers, computer applications to register and track the use of the loudspeakers, and the potential use of artificial intelligence/software agents to automatically activate the pre-recorded messages exclusive of human involvement.

The potential use of artificial intelligence/software agents for CCTV microphones and loudspeakers could also be applied to the video recording capabilities of public surveillance CCTV cameras. For instance, the panoptic feelings, undue surveillance and collateral intrusion brought about by the widespread deployment of public CCTV cameras, which people must involuntarily endure, can be diminished by designing and developing CCTV cameras that only begin to record video when a suspected crime or anti-social act is actually taking place, ignoring ordinary activities and preventing their subsequent scrutiny, as the Royal Academy of Engineering proposes. A software algorithm could be used to process images in real-time and distinguish between suspicious behavior or illegal activities and innocent behavior or legal activities.[856] However, while the use of intelligent software in public surveillance CCTV camera systems is growing, much more intense and difficult research is still required.

There are also PBD solutions for some of the other latest PITs either still in the R&D phase or already deployed and in use. PBD solutions for UAVs include limiting the resolution capability of the video systems and cameras attached to UAVs. PBD solutions for DNA profiles stored on national DNA databases include limiting the creation and exchange of DNA profiles to chromosome zones containing no genetic expression (i.e. not known to provide information about specific hereditary characteristics), as recommended by the Council of the EU.857 PBD solutions for ALPR systems include limiting the vehicle license plate numbers stored on databases connected to an ALPR system to solely those that are being targeted by law enforcement agencies for legitimate purposes, thereby preventing the blanket tracking of the movements of all vehicles. The potential PBD solutions for neurotechnologies, however, are beyond the scope of this dissertation, while possible PBD solutions to minimize the threats to privacy posed by the LEXID® are also uncertain at present time.

856 see Dilemmas of Privacy and Surveillance: Challenges of Technological Change (The Royal Academy of Engineering, London, 2007), p. 42, available at: http://www.raeng.org.uk/news/publications/list/reports/dilemmas_of_privacy_and_surveillance_report.pdf

[857] see Council Resolution of 25 June 2001 on the exchange of DNA analysis results (2001/C 187/01).

9.5 PBD VS. PETS

Similar to the basis of the escalating promotion of data protection through PETs,[858] the benefits of PBD are "premised on the view that it is better to build safeguards in than to bolt them on"[859] and on the valid assumption that it is much more difficult to violate or avoid laws embedded in system code than laws simply written on paper (van Blarkom, G.W. et al., 2003). PETs are technologies that do not threaten privacy, but instead help to protect it by translating 'soft' legal text into 'hard' system specifications (*Ibid*., p. 49). The PISA (Privacy Incorporated Software Agent) project consortium defines PETs as "a system of ICT measures protecting informational privacy by eliminating or minimizing personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system" (*Ibid*., p. 33). PETs mainly comprise of encryption, pseudonymization and anonymization software, firewalls, and other privacy protection tools developed primarily to better ensure the security of personal data. Nevertheless, as initially conceptualized, PETs, like PBD, are also intended to be built into the architecture or fabric of an information system (or technology, device, etc.) at the very outset.[860]

However, while the concept of and premise behind PETs are similar to PBD, PETs and PBD are not the same. PETs are effective (software) technologies or ICT measures, but they can still be circumvented or penetrated, albeit with a level of difficulty that depends on the sophistication of the PET. In addition, anonymization techniques are vulnerable, since anonymized data can be de-anonymized by combining various large datasets and through sophisticated data mining techniques. As Walden points out, "[a]chieving effective anonymisation may be a challenging task, from both a technical and compliance perspective. Sophisticated data analysis and data mining techniques on supposedly anonymous data may eventually yield data that does 'directly or indirectly' relate to a

---

858 see COM/2007/0228 final, Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs); Data Protection Technical Guidance Note: Privacy enhancing technologies (PETs), Office of the Information Commissioner 11/4/06;

859 Williams, Victoria. *Privacy Impact Assessment and the Social Aspects of Public Surveillance* (Evidence for the House of Lords Select Committee on the Constitution inquiry into The Impact of Surveillance and Data Collection upon the Privacy of Citizens and their Relationship with the State), p. 6.

860 see Hes, Ronald. and John Borking (eds.), P*rivacy-Enhancing Technologies: The path to anonymity* (Registratiekamer, The Hague, August 2000), available at: www.cbpweb.nl/downloads_av/av11.pdf
(The groundbreaking work identifies the conditions that should be considered when developing an information system to be privacy-friendly, and clearly presents a few examples of information systems as models for designers/developers, which are meant to be helpful when developing/designing/engineering these types of information systems.)

specific individual, thus rendering it ‘personal data’ subject to the Directive [Directive 95/46/EC]” (Walden, 2002, p. 227). Furthermore, as Walden (2002) additionally points out, “retention of the original data set by a data controller provides the opportunity for any anonymisation process to be reversed at the data controller’s discretion” (*Ibid*.).

On the other hand, the circumvention of PBD solutions is essentially meant to be (practically) impossible or exceptionally difficult, since it would mean attempting to force the device/system concerned to perform an act it is not designed or engineered to do or is not capable of doing (in its present form). The privacy risk or threat of technologies and/or the potential for abuse or misuse of the privacy-intrusive capabilities of PITs by the controllers or operators of these technologies is permanently removed, for the most part, through the regulation and minimization (or elimination) of those risks, threats and capabilities. Thus, PBD aims to design or engineer away, as far as possible, the ability to abuse or misuse the privacy-intrusive capabilities of PITs and to oblige or induce operators/controllers of PITs to appropriately/legitimately use the technologies.[861]

Furthermore, PBD goes beyond PETs. Whereas PETs are *mainly* technical/technological or software-based solutions/ICT measures for protecting privacy and maintaining data security, PBD, as Cavoukian advocates, also includes ‘privacy-friendly’ *both* physical design/architectural solutions and technological/software-based solutions, and business practices/processes and modes of operation.[862] In addition, PBD emphasizes the need to implement PETs, but also requires *privacy by default* settings and the necessary tools to allow users to participate in the protection and management of their personal data (e.g. access controls, user participation tools, etc.).[863] Therefore, PBD is ideally a more comprehensive, holistic approach for avoiding the privacy threats and risks in the first place.

Another difference of PBD solutions from PETs is that the design/architectural and technical solutions are normally unique and tailored to the particular system, technology or device concerned. The solutions can be developed to address specific threats to privacy, beyond the general threats to the privacy and security of personal data, posed by the latest technologies. PETs, on the other hand, are generally homogeneous and are mainly focused on data security.

Moreover, while PETs are often mainly focused on ICT privacy/security issues, PBD, as opposed to PETs, can potentially address the privacy threats of not just ICT, but

[861] For further discussion, see Cavoukian, Ann. Privacy by Design (2009).

[862] see Ann Cavoukian’s “7 Foundational Principles of *Privacy by Design*”, Originally Published: August 2009, Revised: January 2011, available at: http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

[863] For further discussion, see Article 29 Working Party, The Future of Privacy, 1 December 2009, WP 168, p. 13.

also the threats posed by other types of PITs (e.g. imaging technologies), as demonstrated in this dissertation. Hence, PBD does not just apply to IT systems, but may apply to just about any type of device, system, service or technology, albeit to a certain extent.

Finally, PBD can also help to address concerns beyond the protection of privacy/personal data, such as the 'chilling' of the freedom of speech and freedom of movement, and to address other general or specific societal impacts.

9.6 PBD IN THE CURRENT US AND UK/EU LEGAL FRAMEWORKS

While the words "privacy by design" (or "data protection by design") are not specifically found in the current legal framework in the US and UK/EU, and the current data protection legal framework and privacy policies certainly do not seek to influence the basic architecture of computer systems/information technology (Agre and Rotenberg, 1997, p. 3),[864] the role of technical means to protecting privacy, however, can be found in the US and UK/EU legal framework, albeit primarily in the area of data security, rather than for protecting privacy overall.

US legal framework

Within the US, the concept of PBD is briefly found in the Privacy Act 1974. Government agencies are required to:

> establish appropriate administrative, *technical, and physical safeguards* to insure the *security and confidentiality* of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained (emphasis added).[865]

Section 1173 of the HIPAA similarly requires healthcare providers, health plans and healthcare clearinghouses, which maintain or transmit health information, to implement technical and physical safeguards in order to "ensure the integrity and confidentiality of the information" and "to protect against any reasonably anticipated--(i)

[864] But, this may be about to change. Article 23 of the EC's draft proposal for a General Data Protection Regulation (COM(2012) 11/4 draft) is dedicated to "data protection by design" requirements (albeit applicable to data controllers).

[865] Title 5, U.S.C. Part I, Chapter 5, Subchapter II, § 552a (e) (10).

threats or hazards to the security or integrity of the information; and (ii) unauthorized uses or disclosures of the information".

In addition, the Federal Election Commission (FEC) is responsible for issuing Voting System Standards (VSS). For instance, in compliance with The Help America Vote Act of 2002, the FEC issued a VSS to preserve the privacy and confidentiality of the ballot. The VSS, for example, require that all voting booths or enclosures "[p]rovide privacy for the voter, and be designed in such a way as to prevent observation of the ballot by any person other than the voter".[866]

EU legal framework

In the EU, the concept of PBD is found much more frequently within the legal framework. Most significantly, the concept can be found in Directive 95/46/EC, however, the Directive nonetheless does not apply to manufactures or developers. Article 17, paragraph 1 requires that data controllers "must implement appropriate technical and organizational measures to protect personal data". Paragraph 2 of Article 17 further requires that the "controller must, where processing is carried out on his behalf, choose a processor who provides sufficient guarantees in respect of the technical security measures and organisational measures governing the processing to be carried out and must ensure compliance with those measures". Recital 46 requires "that appropriate technical and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing". Schedule 1, Part II, 11 (a) of the DPA identically transposes Article 17 of Directive 95/46/EC into UK law.[867] Moreover, the right of access for data subjects to the "knowledge of the logic involved in any automatic processing of data concerning him at least in the case of the automated decisions", as stipulated by Article 12 of Directive 95/46/EC, could also be considered

[866] Federal Election Commission, Voting System Standards (2002), Volume I, Section 3, § 3.2.4.1 c.

[867] Some EU member states, however, have taken Article 17 a step beyond mainly ensuring data security. Article 13 of Wet bescherming persoonsgegevens (the Netherlands Personal Data Protection Act) requires (unofficial translation provided by the Dutch Data Protection Authority):
The responsible party shall implement appropriate technical and organizational measures to secure personal data against loss or against any form of unlawful processing. These measures shall guarantee an appropriate level of security, taking into account the state of the art and the costs of implementation, and having regard to the risks associated with the processing and the nature of the data to be protected. These measures shall also aim at preventing unnecessary collection and further processing of personal data (emphasis added).

a mechanism for regulating the development of processing systems and better ensuring its transparency.

Article 4.1 of the ePrivacy Directive (Directive 2002/58/EC) requires that a "provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security". Recital 20 further affirms that "[s]ervice providers should take appropriate measures to safeguard the security of their services" and "[t]he requirement to inform subscribers of particular security risks does not discharge a service provider from the obligation to take, at its own costs, appropriate and immediate measures to remedy any new, unforeseen security risks and restore the normal security level of the service". Recital 46 of Directive 2002/58/EC recognized that "[t]he existence of specific rules for electronic communications services alongside general rules for other components necessary for the provision of such services may not facilitate the protection of personal data and privacy in a technologically neutral way" and "[i]t may therefore be necessary to adopt measures requiring manufacturers of certain types of equipment used for electronic communications services to construct their product in such a way as to incorporate safeguards to ensure that the personal data and privacy of the user and subscriber are protected" (emphasis added). Article 14(3) provides that "[w]here required, measures may be adopted to ensure that terminal equipment is constructed in a way that is compatible with the right of users to protect and control the use of their personal data, in accordance with Directive 1999/5/EC and Council Decision 87/95/EEC of 22 December 1986 on standardization in the field of information technology and communications".

Article 3.3(c) of Directive 1999/5/EC,[868] which covers radio equipment and telecommunications terminal equipment, delineates that certain apparatuses may be required to incorporate "safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected".

There is also some case law in the EU relevant to PBD (or *Lex Informatica*). For instance, in Germany the Federal Constitutional Court ruled that the general right of person-

868 Directive 1999/5/EC of the European Parliament and of the Council of 9 March 1999 on radio equipment and telecommunications terminal equipment and the mutual recognition of their conformity

ality (Article 2.1 in conjunction with Article 1.1 of the Basic Law (Grundgesetz – GG)) guarantees the fundamental right to the confidentiality and integrity of IT systems.[869]

Thus, in summary, while there is already a legal basis for PBD in the US and EU, currently this mostly takes the form of PETs and pertains to data security. More importantly, the existing provisions are only applicable to data controllers and/or service providers, with the exception of Article 3.3(c) of Directive 1999/5/EC and Article 14(3) and Recital 46 of Directive 2002/58/EC.

9.7 GROWING WIDESPREAD RECOGNITION

There is a growing recognition in the US and the EU, among privacy experts/legal scholars, governmental bodies, policy makers, data protection/privacy commissioners and NGOs around the world, that PBD is essential to protecting privacy.

While some privacy experts, such as the Information and Privacy Commissioner of Ontario Ann Cavoukian, have long recognized the value of PBD in protecting privacy and have advocated for its widespread adoption, in the past several years, as Gaurda and Zannone (2009) explain, efforts to safeguard privacy have nevertheless still focused on the development of privacy policies, languages, models, standards and user preferences. But, these efforts have offered no practical tools or means for supporting those privacy policies, etc. (Gaurda and Zannone, 2009). However, this could soon change. The efforts to safeguard privacy are indeed gradually moving towards the focus on developing those practical tools and means/measures.

In a policy paper, the European Data Protection Supervisor (EDPS) Peter Hustinx affirmed, "privacy and data protection requirements need to be highlighted and applied as soon as possible in the life cycle of new technological developments in order to contribute to a better implementation of the data protection legal framework".[870] The EDPS further added, "the European RTD [research and technological developments] efforts constitute a very good opportunity to accomplish these goals and the EDPS considers that the principle of '*privacy by design*' should represent an inherent part of these RTD

[869] BVerfG, 1 BvR 370/07 vom 27.2.2008, Absatz-Nr. (1 - 267), available at: http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html
For further discussion on the significance of the German ruling for Lex Informatica, see Cannataci, Joseph A. *Lex Personalitatis: Personality, Law and Technology in the 21st Century* (Acta Universitatis Lucian Blaga 219, 2008).

[870] EDPS and EU Research and Technological Development, Policy paper, Brussels, 28 April 2008, p. 2.

initiatives”.[871] The EDPS Peter Hustinx has continued to be an important supporter and outspoken promoter of PBD in the EU.[872]

In line with this policy, the EC has indeed funded a number of relevant projects to help integrate privacy, human rights, legal, social and ethical considerations and discourse into research and technological development. Projects, such as, DISCREET, PISA, PRIME and PrivacyOS, are aimed at developing the technical means to protecting privacy, albeit more related to PETs and middleware solutions as opposed to wide-ranging PBD solutions and architectures. Project DETECTER, however, specifically aims to positively influence the design and development of detection technologies (biometrics, video surveillance, GPS, RFID and audio-bugging), which are used in counter-terrorism activities, by engaging in dialogue with the manufacturers and users of these technologies on human rights standards. The ICTETHICS project aims to develop an integrated non-technical approach to addressing the ethical, legal and social aspects of ICT. The PRACTIS project aims to assess the potential impacts on privacy from emerging technologies, such as nanotechnology, biotechnology and neurotechnology, and explore methods of embedding privacy considerations in the development process of new technologies. The ETICA project aims to identify ethical issues arising from ICT in the coming 10-15 years. In addition, the PRESCIENT[873] project also “aims to provide an early identification of privacy and ethical issues arising from emerging technologies and their relevance for EC policy”.[874]

In an earlier opinion on better implementing the Data Protection Directive, the EDPS recommended that measures to better comply with the data protection principles should “build on the concept of ‘privacy by design’, ensuring that the architecture of new technologies is developed and constructed by taking properly into account the principles of data protection”.[875] The EDPS further added that “[t]he promotion of privacy-compliant technological products should be a crucial element in a context in

[871] *Ibid.*

[872] In his closing speech at the third annual international conference *Computers, Privacy and Data Protection* on January 29-30 2010 in Brussels, I was glad to especially hear the EDPS emphasize the important need to begin regulating manufacturers of ICT for the sake of privacy.

[873] An acronym for: “Privacy and Emerging Sciences and Technologies”

[874] Prescient project, available at: http://www.prescient-project.eu

[875] Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive (2007/C 255/01), para. 63.

which ubiquitous computing is fast developing".[876] The EDPS also explicitly stressed, once again, the utmost importance of implementing PBD in practice and integrating PBD into the EU legal framework.[877]

As a result, the EDPS has strongly stressed, on numerous occasions, the critical significance of PBD to defend against the ubiquitous nature of RFID applications, calling for the "mandatory deployment of RFID applications with the appropriate technical features or 'privacy by design'".[878] The EC has agreed and equally expressed its belief that "privacy and information security features should be built into RFID applications before their widespread use (principle of 'security and privacy-by-design')".[879] However, while the EC recommends the use of PBD to help implement privacy and data protection principles in RFID applications, the recommendations are again exclusively focused on the providers of those applications and the related data controllers, and not the developers/manufacturers of RFID tags and readers.

Earlier this year, European Commissioner for Justice, Liberty and Fundamental Rights, Viviane Reding, announced plans to strengthen the Data Protection Directive by requiring that new technologies and processes include PBD, noting that privacy and data protection are not always considered during the development of ICT products and services and calling for this shortcoming to be remedied.[880] Much more broadly, the EC has also fully endorsed PBD as a component of Europe's forthcoming Digital Agenda by affirming that PBD must be widely applied within relevant ICT technologies, in order to effectively enforce the right to privacy and the protection of personal data.[881]

---

876 *Ibid.*

877 see Opinion of the European Data Protection Supervisor on Promoting Trust in the Information Society by Fostering Data Protection and Privacy, 10 March 2010.

878 see Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on 'Radio Frequency Identification (RFID) in Europe: steps towards a policy framework' COM(2007) 96 (2008/C 101/01).

879 C(2009) 3200 final, Commission Recommendation of 12.5.2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification.

880 "EU Commission outlines plans to strengthen privacy law" (OUT-LAW News, 29 January 2010), available at: http://www.out-law.com/page-10712

881 see Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of Regions, A Digital Agenda for Europe, COM(2010) 245.

Indeed, the EC's proposal for an EU General Data Protection Regulation[882] has dedicated an entire article to PBD, requiring data controllers to "implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not be collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage"[883] and empowers the EC to adopt delegated acts for the purpose of specifying the requirements for appropriate measures/mechanisms for implementing *data protection by design* applicable for products and services.[884]

The Article 29 Working Party previously weighed in heavily. In a widely acclaimed position paper on the "Future of Privacy", adopted in December 2009, the advisory body explicitly endorses the view that PBD is one of the critical requirements for protecting privacy in the future, and recommends that the revision of Directive 95/46/EC should be innovative by introducing provisions on PBD. PBD is required, the Article 29 Working Party argues, in order to "counterbalance" the risks to individual privacy posed by the latest technological developments. Most significantly, the position paper affirms that PBD requirements for ICT should be binding not just for data controllers, but also for technology designers and producers.[885] The Article 29 Working Party also essentially points out that while Article 17 and Recital 46 of Directive 95/46/EC are helpful towards the promotion of PBD, in practice these provisions are insufficient. There was, however, a missed opportunity to more clearly stress that PBD goes beyond PETs, and should be deeply rooted in the physical architecture and overall design of *any* device or system.

In the *Report to Congress regarding the Terrorism Information Awareness Program*, written by DARPA, the significance of built-in safeguards to reduce potential abuse of technologies capable of mass surveillance was highlighted. The report listed safeguards such as regulating the research and development of surveillance technologies and implementing security measures to prevent unauthorized access (2003, pp. 33-35).

The DHS Privacy Office has developed the official guidance, *Privacy Technology Implementation Guide* (PTIG), which is a procedural guide for technology managers and developers on how to integrate privacy protections in the early stages of the devel-

---

882 see Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11/4 draft.

883 *Ibid*., Article 23, para. 2.

884 *Ibid*., Article 23, para. 3.

885 Article 29 Working Party, The Future of Privacy, 1 December 2009, WP 168, p. 13.

opment of IT systems that collect, process, or produce personal data. In addition, the FTC published a Staff Report, titled "Protecting Consumer Privacy in an Era of Rapid Change", which emphasizes the potentially important role of PBD.[886]

A conference held by the UK's ICO on PBD and its accompanying report clearly recognized the merits of PBD.[887] In another report, the Royal Academy of Engineering affirmatively expressed the value in 'designing for privacy' and recommended both technical and legal solutions to some of the new privacy dilemmas we face today.[888]

The international conferences of data protection and privacy commissioners have also consistently supported the development and implementation of PBD. For instance, at the 31st International Conference of Data Protection and Privacy Commissioners in Madrid, a workshop on PBD was held and attended by numerous distinguished experts and officials, and at the 32nd International Conference of Data Protection and Privacy Commissioners a Resolution on Privacy by Design, declaring PBD as an essential component of fundamental privacy protection, was endorsed by data protection/privacy commissioners around the world.

In a letter to Chairman and CEO of Google, Eric Schmidt, signed by the heads of nine data protection authorities from different parts of the world, including the Chairman of the Article 29 Working Party, Jacob Kohnstamm, the sponsors called upon Google, and all other organizations entrusted with personal information, "to incorporate fundamental privacy principles directly into the design of new online services".[889]

Moreover, a growing number of authors are also arguing in favor of focusing on technical solutions to enforce privacy policies and laws, as opposed to relying merely on humans to do so (see, e.g., Karat et al., 2005; Leenes and Koops, 2005; Albrechtslund, 2007; Gaurda and Zannone, 2009; Hildebrandt and Koops, 2010).

---

886 As a follow-up to the preliminary FTC Staff Report, the FTC Final Report, "Protecting Consumer Privacy in an Era of Rapid Change", was published in March 2012, available at: http://ftc.gov/os/2012/03/120326privacyreport.pdf

887 Privacy By Design Report, Information Commissioner's Office, 2008, available at: http://www.ico.gov.uk/upload/documents/pdb_report_html/privacy_by_design_report_v2.pdf

888 see Dilemmas of Privacy and Surveillance: Challenges of Technological Change (The Royal Academy of Engineering, London, 2007), available at: http://www.raeng.org.uk/news/publications/list/reports/dilemmas_of_privacy_and_surveillance_report.pdf

889 The letter, dated April 19, 2010, is available at: http://www.priv.gc.ca/media/nr-c/2010/let_100420_e.pdf

9.8 POTENTIALLY GROWING APPLICATION

Data controllers are increasingly using PETs, as revealed by a Eurobarometer survey conducted in 2008. According to the survey, 52% of data controllers interviewed throughout the EU stated that they have used PETs (e.g. encryption tools and anonymization software) for enhancing the privacy protection of their databases, which, in comparison with the survey results of 2003, is a substantial increase.[890] This increase is perhaps partly due to their increased awareness of PETs. Nevertheless, while the increased usage of PETs is certainly welcoming, the survey results show that half of all data controllers still do not use PETs. However, the next survey may reveal further increase in the use of PETs.

As explained earlier, PBD goes beyond PETs, so the survey does not provide empirical evidence on the scope of PBD use. However, the employment of PBD solutions does already exist in different ways, albeit subtly and not so clearly. For example, ATMs are already designed to take into account privacy requirements[891] and voting booths are also developed to better ensure the privacy of one's vote. Facebook, while far from perfect, has also (partially) adopted a PBD approach by allowing users to more easily select their account settings for sharing their information and by allowing users to access an expanded data archive on their account history. Google's "dashboard" and default settings may also be another example of PBD. But, the solutions for Facebook and Google could potentially be removed or backtracked altogether, and are more like PETs than PBD. The adoption of the opt-in approach and the use of privacy-friendly settings by default for a number of devices and digital services are also examples of PBD. And, the already deployed software solutions for body scanners to protect privacy and the remote separation of the console, where the images are viewed from where the passengers are scanned, are other potential examples. Still, many of these PBD solutions deployed are not externally certified and the law does not mandate nor encourage their deployment.

---

[890] see Flash Eurobarometer No 226, Data protection perceptions among data controllers, survey conducted by The Gallup Organization Hungary upon the request of the Directorate-General Justice, Freedom and Security of the European Commission, Analytical Report, February 2008.

[891] see Little, Linda., Pam Briggs and Lynne Coventry. *Public space systems: Designing for privacy?* (International Journal of Human-Computer Studies, Volume 63, Issues 1-2, July 2005), pp. 254-268.

9.9 LACK OF TRUST

The recognition in the value of PBD might have something to do with the public's lack of trust in governments, companies, data controllers and their agents to deploy and use PITs ethically, justifiably and in accordance with the law and fundamental principles of privacy. For example, we are increasingly learning of the misuse of access to the vast quantities of personal data stored on databases by government/law enforcement agents and of the deception of certain companies regarding the collection and use of location information.

As a result, there are valid points of view that we are more likely better-off relying on the ability to control technological development in a way that safeguards the right to privacy, rather than only attempting to control individuals to comply with privacy laws/principles.[892] As Masters and Michael (2006) point out, "given that humans do not by nature trust others to safeguard their own individual privacy, in controlling technology we feel we can also control access to any social implications stemming from it" (2006, p. 37). Interestingly, in the words of former Federal Reserve Chairman, Alan Greenspan, "[i]ndeed, the most effective means to counter technology's erosion of privacy is technology itself".[893]

These assumptions are re-enforced by the public's potentially growing lack of trust in governments and companies to safeguard their right to privacy. The consequence of this may also have detrimental effects on the legitimacy of governments, which will likely only become worse as PITs further evolve and their deployment expands.

It is also widely accepted that trust is key to economic growth and prosperity (RISEPTIS Report, 2009, p. 14). As a Booz & Company 2008 study similarly affirms:

> The difference between "getting Digital Confidence right" in a best-case scenario and "getting it wrong" in a worst-case scenario adds up to €124 billion, or almost 30 percent of the total market at stake—approximately 1 percent of total EU-27+2 GDP in 2012! The combined downside of failing to establish Digital Confidence is, at €78 billion, far greater than the upside at €46 billion—primarily driven by the effects of Privacy and Data Protection as well as Network Integrity and Quality of Service, which impact all the revenue

---

892 see Masters, A. and K. Michael. L*end me your arms: the use and implications of humancentric RFID* (Faculty of Informatics, University of Wollongong, 2006).

893 Alan Greenspan's words at a Conference on Privacy in the Information Age (Salt Lake City, 7 April 1997), available at: http://www.federalreserve.gov/boardDocs/speeches/1997/19970307.htm

areas of the digital economy and the level of use and number of users across the major revenue categories.[894]

Therefore, the growing lack of trust in companies to ensure privacy, data protection and data security will increasingly result in missed business opportunities and sluggish innovation (Williams, 2009, p. 78). In the long run, this lack of trust could seriously impact the bottom-line of companies.

9.10 A UNIQUE SELLING POINT

Although up until the late 1990s relatively "little work has been done to evaluate the economic impact of privacy policy" (Agre and Rotenberg, 1997, p. 22) or to study the "economics of privacy"[895] or to explore how privacy can be monetized, since then the topic has indeed grown into its own area of specialty.[896]

There is now a growing understanding that privacy can overall help the bottom-line of companies.[897] In addition, it is now increasingly recognized that companies can potentially improve the trust of their customers by safeguarding their privacy, thereby improving their reputation and image (Borking, 2010). By implementing PBD measures and/or engaging in other privacy-friendly practices, companies can also reduce their

---

[894] *Digital Confidence – Searching the next wave of digital growth* (Booz & Company, Liberty Global Policy Series, 2008), p. 9.

[895] see Posner., Richard. *The economics of privacy* (American Economic Review, Vol. 71, Issue 2, 1981), pp. 405-409; Posner, Richard. A*n economic theory of privacy* (Regulation, 19-26, 1978).

[896] see, e.g. Taylor, Curtis R. *Private demands and demands for privacy: Dynamic pricing and the market for customer information* (Technical report, Department of Economics, Duke University, 2002); Acquisti. Alessandro. "Security of Personal Information and Privacy: Technological Solutions and Economic Incentives" in J. Camp and R. Lewis (eds.), *The Economics of Information Security* (Kluwer, 2004). For additional examples of papers/books on the "economics of privacy", see Acquisti's academic website at: http://www.heinz.cmu.edu/~acquisti/economics-privacy.htm

[897] John Borking, for instance, has conducted significant research on the costs of privacy risks for businesses and quantifying the economic justifications for organizations to invest in privacy risk-reducing technical solutions, such as PETs. see Borking, John. "Assessing investments mitigating privacy risks" in Laurens Mommers, Hans Franken, Jaap van den Herik, Franke van der Klaauw and Gerrit-Jan Zwenne (eds.) *Het binnenste buiten; Liber amicorum ter gelegenheid van het emeritaat van Prof.dr.Aernout H.J.Schmidt, Hoogleraar Recht en Informatica te Leiden* (eLaw@Leiden, 2010), pp. 255-273.

risk of legal liabilities[898] and prevent potentially bad publicity. Basically, in the words of Harriet Pearson, IBM's Chief Privacy Officer, "privacy is good for business".[899]

Just as companies are increasingly realizing that "going green" and designing and manufacturing products in an environmentally-friendly manner is good for business and the investment of doing so will pay off in the long-run, so too are companies increasingly realizing that designing technologies in a privacy-friendly manner could drive their business forward and provide the products and services that both governments and consumers demand.[900]

Indeed, there is a business case for privacy-friendly practices and commercial/economic benefits and competitive advantages for companies that implement PBD solutions and PETs.[901] As Rob van Kranenburg pointed out, PBD "is not only culturally and socially productive but business wise fostering privacy as a *unique selling point*" (emphasis added).[902] The recognition that engaging in privacy-friendly practices may also be part of a marketing strategy might explain the fact why marketing managers for data controllers were actually the respondents, of a 2008 Eurobarometer survey, most likely to say that their company used PETs.[903] In short, as "going green" is increasingly translating into profit, being privacy-friendly could also increasingly mean legal stability, profitability and marketability for companies in the long-run.

898 see Holmes, Allan. *The Profits in Privacy* (CIO Magazine, 15 March 2006), available at: http://www.cio.com/article/19070/The_Profits_in_Customer_Privacy

899 see an interview with IBM's Chief Privacy Officer Harriet Pearson, available at: http://www.03.ibm.com/innovation/us/customerloyalty/harriet_pearson_interview.shtml

900 For example, Hewlett-Packard (HP) has recognized the value of PBD for business. see *Privacy by Design: Essential for Organizational Accountability and Strong Business Practices*, (November 2009), co-authored by Scott Taylor (Chief Privacy Officer of HP), Ann Cavoukian (Information & Privacy Commissioner, Ontario, Canada) and Martin E. Abrams (Senior Policy Advisor and Executive Director, Centre for Information Policy Leadership, Hunton & Williams LLP).

901 John Borking, for instance, has also conducted research on the economic benefits of PETs. see Borking, John. "Assessing investments mitigating privacy risks" in Laurens Mommers, Hans Franken, Jaap van den Herik, Franke van der Klaauw and Gerrit-Jan Zwenne (eds.) *Het binnenste buiten; Liber amicorum ter gelegenheid van het emeritaat van Prof.dr.Aernout H.J.Schmidt, Hoogleraar Recht en Informatica te Leiden* (eLaw@Leiden, 2010), pp. 255-273.

902 van Kranenburg, Rob. The Internet of Things: *A critique of ambient technology and the all-seeing network of RFID*, Network Notebooks 02, Institute of Network Cultures (2008), p. 49, available at: http://www.networkcultures.org/_uploads/notebook2_theinternetofthings.pdf

903 see Flash Eurobarometer No 226, Data protection perceptions among data controllers, survey conducted by The Gallup Organization Hungary upon the request of the Directorate-General Justice, Freedom and Security of the European Commission, Analytical Report, February 2008.

9.11 POTENTIAL CRITICISM

A number of legal authors/scholars have, to some extent, criticized Lessig's "code as law" for various reasons. The concept is certainly not immune to criticism.

Gutwirth et al. (2008) essentially argue that Lessig disregarded the politics, dynamics and complexity of lawmaking and how legal practitioners and courts operate in the real world. They also question the viability of achieving an "optimal mix" of Lessig's four dimensions/modalities of regulation.[904]

Schwartz (2000) also criticizes Lessig's concept of "privacy-control", arguing that "privacy-control seeks to place the individual at the center of decision making about personal information use, but it can instead help us to accept smoke screens that disguise information privacy practices and lead to choices that are bad for individuals and for society".[905] Schwartz argues that Lessig's "technological solution, privacy-code, which relies on measures such as P3P, is likely to form such a smoke screen".[906]

Schwartz (2000) further questions the effectiveness of over relying on individual control of personal data to reach optimal levels of privacy, as a result of 'market failures' and failures of private agreements.[907] Schwartz argues, "due to the extent of the failure in the privacy market, the law at present should generally seek to minimize harms that flow from reliance on bargaining among consumers and data processors".[908] Moreover, Schwartz (2000) rightfully points out that Lessig's approach to individual privacy control is mostly not relevant for law enforcement purposes, since law enforcement agencies are generally not required to obtain permission to carry out surveillance operations.[909]

As values, norms or rules are increasingly being built into technology, some authors, including, for example, Koops (2007), have questioned the compatibility of the "code as law" and PBD approach with the democratic system, if not sanctioned by

---

904 Gutwirth, Serge., Paul De Hert,. and Laurent De Sutter. "The trouble with technology regulation from a legal perspective. Why Lessig's 'optimal mix' will not work" in Brownsword, R. and Yeung, K. (eds.) *Regulating Technologies* (Hart Publishers, 2008), pp. 193-218.

905 Schwartz, Paul M. *Beyond Lessig's code for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices* (Wisconsin Law Review, Volume 2000, Issue No. 4, 2000), pp. 743-787, at 760.

906 *Ibid.*

907 *Ibid.*, p. 782.

908 *Ibid.*

909 *Ibid.*, p. 784.

elected representatives in accordance with the law.[910] Indeed, "code as law" may arguably be one way of bypassing regular democratic procedures of lawmaking and/or law enforcement to regulate or restrict human behavior and activities. Computer programmers/engineers, in this sense, could theoretically become the new lawmakers of the 21st Century, acting at the request of either corporations or governments.

Additional criticism of PBD may come from those who argue that such an approach to regulating technological development may stifle innovation. For further discussion on why this argument, while not without merit, overlooks the potential benefits of PBD on promoting deployment and innovation of future and emerging technologies through the increased trust and confidence of consumers/citizens, see section 10.13.

9.12 PRACTICAL CHALLENGES OF IMPLEMENTING PBD

In addition to the criticism of PBD, the practical challenges of implementing PBD and embedding the fundamental principles of privacy into the design/architecture of ICT and other PITs in reality should also not be ignored. Evidently, 'translating' written legal norms/principles into design solutions/computer code or bridging the significant differences between legal (natural) language and computer/machine language is a challenge.[911] Indeed, the extent to which legal protection can be programmed, engineered or automated is open to discussion, and there is currently no single widely accepted methodology or approach for translating privacy/data protection laws into technological/design solutions.

First of all, it is difficult to balance the need for specificity with the benefits and needs of flexibility (see section 10.5 for further discussion on flexibility vs. specificity). There are some benefits from the flexibility and ambiguity often intrinsic in natural language, which will be forgone due to the specificity and rigidity of machine/computer language. As Grimmelmann argues, "[b]ecause a computer, rather than a person, makes a program's decisions, rules encoded in software are free from ambiguity, discretion, and subversion" (2005, p. 1723). The challenges generally concern the flexibility of human interpretations and understanding of natural language, and how this also differs or conflicts with the rigidity of machine/computer language interpretation (for further

910 see Koops, Bert-Jaap. *Criteria for Normative Technology: An Essay on the Acceptability of 'Code as Law' in Light of Democratic and Constitutional Values* (Tilburg University Legal Studies, Working Paper No. 007/2007, 2007).

911 For further discussion, see Guarda, Paolo., and Nicola Zannone. T*owards the development of privacy-aware systems* (Information and Software Technology, Volume 51, Issue 2, February 2009), pp. 337-350.

discussion, see, e.g., Grimmelmann, 2005). For instance, lawmakers/legal practitioners may interpret or understand the legal norms/privacy principles differently, given the lack of overall consensus on what constitutes privacy, and these interpretations may also change over time (see section 2.2 for further discussion), causing the 'translation' to be further complex. And, "[a]s the complexity of particularized rules increases, their formal realizability decreases" (Grimmelmann, 2005, p.1733). Technology/design-based solutions work best for areas/matters where there is a consensus on meanings, but is certainly more challenging where there is significant disagreement (Yeung and Dixon-Woods, 2010).

In addition, some of the legal norms/privacy principles may not be specific or detailed enough, which may call into question the ability of programmers/engineers to effectively develop/implement PBD solutions for realizing the privacy principles/legal norms in a methodical and consistent way.[912] As Grimmelmann explains, when "a programmer attempts to envision as precisely as possible the details of the process by which she would like that task carried out. This precision is necessary because she must express her intention in the text of a computer program — a list of instructions, written in one of a number of artificial languages intelligible to a computer. Compared with human languages, these languages are highly constrained. Each of her instructions carries a fixed and precise meaning" (2005, p. 1728).

Therefore, the PBD requirements will need to be detailed and precise enough, in order to equally ensure that developers/manufacturers are able to clearly identify or determine what is specifically required.[913] Then, developers/manufacturers/engineers will also be better able to develop/implement specific, concrete PBD-based solutions for complying with these specific requirements and norms, while still taking into consideration the specific characteristics and privacy threats/risks of different devices, systems or technologies concerned. Equally, the principles of privacy and other legal privacy norms will also need to be as specific as possible, in order for computer programmers to effectively codify the principles/norms through computer code. Nevertheless, as Grimmelmann also points out, even the most precise rules could still provoke a certain degree of discretion and facts are still vulnerable to preconceptions and other "non-legal sensibilities" (Grimmelmann, 2005, p. 1733).

But, while specificity is required, at the same time, it is clear that PBD legislation and the concept of PBD will also need to be technologically neutral, goal-orientated

[912] see Pasic, Aljosa. "Privacy by Design: An industry perspective on the challenges and opportunities of privacy", available at: http://www.eurescom.eu/?id=531

[913] *Ibid.*

and general or flexible enough to ensure that all technologies, devices, systems, etc. and domains are covered. Also, the PBD requirements will need to be flexible enough to allow and encourage the development of innovative PBD solutions. It will be challenging to find the right balance.

Furthermore, the success and utility of the development and implementation of the required technical and design solutions is also dependent on the means, abilities, capacities and resources of the developers/manufacturers. The implementation of PBD equally depends on the availability of the required skills and know-how of programmers/engineers.[914] Undoubtedly, the development of certified-compliant PBD solutions and certified engineers/programmers will be a lengthy and complex process and will demand substantial investment and dedicated resources.[915]

In order to support developers/manufacturers to even begin to overcome these challenges, a variety of steps, actions and measures will need to be carried out (see section 10.17).

9.13 CONCLUDING REMARKS

The benefits and value of PBD are now increasingly recognized or apparent. But, PBD is not a panacea for defending privacy and the concept is certainly not immune to criticism. In addition, the significant challenges and difficulties of legislating for PBD, implementing/enforcing PBD and monitoring, measuring or assessing its effectiveness cannot be overlooked.

914 *Ibid.*

915 For further discussion, see *Ibid.*

PART IV

10 Overall conclusions & policy recommendations

10.1 CHAPTER INTRODUCTION

Section 10.2 outlines the challenges lawmakers face in order to keep up with technological development. Section 10.3 further explains how PBD, as the critical combination of law and technology, is a solution. Section 10.4 clarifies that PBD is not a substitute for law. Section 10.5 explains the need to balance flexibility with specificity. Section 10.6 proposes PBD legislation as a radical solution to counter the radical capabilities of the latest PITs. Section 10.7 and Section 10.8 provides an overview of the mechanisms and steps for implementing and enforcing the proposed legislative solution. Section 10.9 proposes a certification-scheme for PBD. Section 10.10 explains the requirements for designing for privacy, while Section 10.11 outlines what constitutes adequate PBD. Section 10.12 outlines the negative effects of overregulation and overprescribing the PBD solutions. Section 10.13 argues how PBD could increase the deployment and innovation of technologies. Section 10.14 sums up how PBD can jointly safeguard and enhance privacy, liberty and security in the 21st Century. Section 10.15 clarifies the continued need for privacy-friendly alternatives, regardless of PBD. Section 10.16 counters some potential criticism of PBD. Section 10.17 outlines some recommendations to overcome the practical challenges of PBD. Section 10.18 explains the need to engage stakeholders and other relevant actors to further overcome the challenges and realize the potential of PBD. Section 10.19 clarifies that PBD, while it may be an effective solution, is not a panacea. Section 10.20 sums up the final overall conclusions of the dissertation.

The overall problems, root causes, objectives, recommendations and countermeasures addressed by this dissertation are mapped out and summarized in an *A3 Report* (see: Annex I). Once again, it is important to note that the A3 Report was developed only after the overall research findings and conclusions were established. Moreover, the overall conclusions, which are elaborated in more detail and brought into focus in the subsequent sections, are based on the analysis and conclusions from the case studies.

An overview of the intrusive capabilities of the specific PITs addressed and the corresponding most relevant laws and self-regulations, legal deficiencies, and proposed key recommended legal and technological solutions are outlined in a summary table (see: Annex II).

10.2 KEEPING UP WITH THE TECHNOLOGY.

PITs, with ever-greater intrusive capabilities, will likely always evolve faster than privacy/data protection laws. The speed of lawmaking has essentially been (and will likely continue to be) slow, while the speed of technological development, innovation and deployment has been increasingly rapid. A single innovation can lead to multiple innovations, which in turn can lead to exponentially more innovations. And, for every new, innovative PIT developed/deployed, the law is even further behind the technology.

Privacy/data protection laws, applicable only to data controllers and users of PITs, are probably much less able to withstand the new technological developments. However, the rapidly changing and advancing nature of technology is not a justification for not being able to equip the law with the practical means of standing a better chance of adequately defending the right to privacy and other civil liberties. For far too long, the difficulty of keeping up with technology has brought some doubt over the ability of lawmaking/policymaking to do something concrete to ensure privacy. This skepticism has also perhaps partially led to politically delegitimizing or foiling, especially in the US, legislative attempts to pass new and comprehensive privacy laws.

On the other hand, as demonstrated through the case studies, privacy/data protection laws, directly applicable to the manufacturers/developers of PITs, are better suited to more effectively safeguard privacy and liberty against the threats posed by existing technologies and future and emerging technologies. But, before the adoption of new policies and laws can be achieved, lawmakers and policymakers need to be influenced and convinced, through concrete solutions and validated real-life demonstrations, that privacy can be engineered into PITs. By providing the actual ability to take concrete steps, PBD can offer the necessary preconditions for addressing privacy concerns on a political and economic level (Agre and Rotenberg, 1997).

10.3 PBD: A CRITICAL COMBINATION OF TECHNOLOGY AND LAW

Privacy is not just a policy, theoretical or legal issue that can be maintained with purely legal or policy-orientated solutions. Privacy laws are only as good as the controls, means or measures for implementing those laws and, therefore, in order to realize the promise of the privacy laws, the practical implementation is required. If not effectively implemented, law, no matter how strict or comprehensive, is just a 'paper tiger'. As the Article 29 Working Party similarly argues, "[d]ata protection must move from 'theory to practice'. Legal requirements must be translated into real data protection measures".[916] Or, as Reidenberg (2000) argues, "law is necessary to establish the public policy objectives, but insufficient to assure the implementation of fair information practices".

The minimization of the threats/risks posed by the highly intrusive capabilities of PITs will likely continue to prove farfetched and difficult to realize, without practical measures and by relying solely on the behavior of people to comply with the law and to appropriately use PITs. After all, no matter how strict and comprehensive privacy laws are formulated and how unambiguously the right to privacy is delineated and interpreted, there will always be attempts to violate those laws and infringe upon the right to privacy. In response, practical measures in the form of technological and design (PBD) solutions can bolster the law and better ensure or even almost guarantee its compliance. Solutions or fixes based on technology, code and architectures are, therefore, critical.

Essentially, in terms of privacy and other civil liberties, technology can be both a threat and a solution. In other words, technology can provide the powerful instruments of surveillance and privacy intrusion, but also the effective controls over these activities. For all four PITs (i.e. case studies) specifically addressed, technical or design solutions/measures played an important, often essential, role in regulating and minimizing the threats to privacy and individual liberty. Indeed, the proposed recommendations to enhance the legal frameworks in the US and UK are based heavily on technological or design solutions for implementing existing privacy principles and laws, and the creation of new laws that require these solutions be implemented.

For body scanners, it is essential that the devices do not generate images that are unnecessarily graphic, which can be accomplished using software algorithms, and that the devices have restricted storage capabilities. For CCTV microphones, it essential that the technology used is not capable of recording conversations out in public, without first being legitimately triggered by certain sounds using artificial intelligence. For CCTV loudspeakers, it is essential that their design does not give control room opera-

[916] Article 29 Data Protection Working Party, WP 173, Opinion 3/2010 on the principle of accountability, 13 July 2010, p. 3.

tors the capability to say whatever they want from afar and out loud. It is also important that their use is automatically tracked and logged. And, for HIMs, marketed and sold for human implantation, without technological approaches, protecting the privacy of RFID or GPS implantees will be incredibly difficult. It is essential that RFID implants possess strong encryption and it is important that the privacy principles are incorporated at the "reader-to-tag protocol level". It is also important that implantees are able to set 'privacy preferences', where appropriate, which is only possible through technological approaches.

Furthermore, the ubiquitous information society, which HIMs and other RFID applications could form a key part of, will bring about difficulties to preserve privacy without PBD solutions or built-in privacy awareness (see Langheinrich, 2001). PBD will especially be imperative in a ubiquitous information society, where it will likely prove difficult to determine all the responsible entities and to enforce privacy/data protection laws in the traditional way. PBD will also be evermore important as ICT becomes increasingly pervasive and entrenched within society and everyday life, from the deployment of smart electricity meters and smart electricity distribution grids[917] to e-health, e-commerce and e-government applications.

Privacy is just too important to solely rely on operators of PITs and data controllers to uphold the principles of privacy. Technology more than likely can do a better job. Operators and data controllers comply with privacy laws and principles irregularly, inconsistently, subjectively, manually and with errors. Operators or controllers, whether private or public, and service providers are either prone to make mistakes in handling personal data or are prone to abuse or misuse the powerful intrusive capabilities of PITs, both of which have reportedly occurred countless times, not to mention those incidents that have gone unreported. Technology, on the other hand, in theory, can apply privacy laws and principles constantly, consistently, objectively, mechanically and without errors, improving both the rate and quality and effectiveness of privacy compliance. Rather than solely regulating the ways in which the capabilities of technology is used, with PBD those capabilities are regulated and minimized in the first place.

In addition, as the Article 29 Working Party again similarly points out, data controllers (i.e. private enterprises and public sector bodies) are often merely users of ICT and

917 The white paper from the Future of Privacy Forum, *SmartPrivacy for Smart Grids: Embedding Privacy into the Design of Electricity Conservation* (November 2009), argues in favor of implementing PBD for smart grids and warns about the threats to privacy posed by smart grids. For example, as the white paper points out, by revealing what appliances and devices a household uses, how much and when, the electricity provider can determine personal habits, behaviors and lifestyles. There are indeed legitimate privacy concerns surrounding smart grids that should not be simply overlooked, but the full privacy implications of smart grids are unknown, and therefore PBD here is a key preventive measure.

can hardly be considered in a position to take any relevant security or data/privacy protection measures by themselves even if they wanted to.[918] More appropriately, therefore, requirements should fall on the ICT manufacturers/developers.

Besides, in an emerging ubiquitous information society, where ICT deployment and use is increasingly pervasive, it will only become even harder to know who are all the data controllers and, thus, more difficult to always determine who should be held accountable. The enforcement and effectiveness of privacy laws, like in any legal field, requires the capacity to allocate responsibility to the appropriate parties for complying with the relevant regulations and to hold those accountable who fail to comply. Therefore, not being able to determine the responsible data controllers in an increasingly ubiquitous information society will substantially weaken the function and meaning of the privacy laws and principles.

Shifting the focal point of obligations to the developers/manufacturers of PITs and putting less weight on the operators and data controllers is also particularly important in public surveillance terms, for example with regards to CCTV microphones and loudspeakers and RFID/GPS implants, since there seems to be no clear way of determining the extent to which privacy exists in public, especially when public surveillance technologies are so widespread and many argue that there is no privacy out in public. Furthermore, PBD will become even more critical as the deployment of ubicomp, AmI and the Internet of Things/Internet of Persons becomes a reality causing the extreme difficulty of implementing the legal requirements and the privacy principles, such as the principles of consent/choice and notice/awareness, within public settings. Essentially, exercising choice in an unregulated (or inadequately regulated) ubiquitous information society means making a decision between going out in public or staying home or becoming a "digital hermit",[919] and this is not really a choice at all.[920]

PBD is also especially critical for protecting privacy in a world of increasing cross-border data flows, for example, as a result of the increase in 'cloud computing', global databases and online social networks. This problem is especially accentuated, since different legal jurisdictions have different degrees of adequacy in data protection rules. As Reidenberg (2000) points out, "the inevitability of conflict between comprehensive legal standards, as found in Europe, and ad hoc protections, as seen in the United States, place the issue of fair treatment of personal information at the center of global information

---

918 see Article 29 Working Party, The Future of Privacy, 1 December 2009, WP 168.

919 see Cave, J., et al. *Trends in connectivity technologies and their socio-economic impacts*, Final report of the study: Policy Options for the Ubiquitous Internet Society, (RAND Europe, July 2009), p. 19.

920 *Ibid.*

transfers". PBD can better ensure the consistent protection of personal data, to a certain extent, regardless of geographic location, legal jurisdiction or the adequacy of the legal framework, since "mechanisms that automate the implementation of data policies will facilitate uniformity across the areas of law and marketplace" (Reidenberg, 2000).

Therefore, in summary, PBD is imperative when the legal questions are left wide open, the legal solutions are ambiguous or extremely difficult to enforce/implement or when essentially there are no applicable laws or those laws are inadequate.

Nevertheless, at present the technical emphasis, found both in law and industry standards (such as ISO/IETF 27000-series, ISO/IEC 17799:2005(E) and ISO/IEC 13335-1:2004), is all too often focused on data security. While data security is an important element in privacy protection, it is just one principle of protecting privacy and not the whole picture. As a result, there is a lack of guidance, rules and established industry standards on the technical solutions to ensuring privacy overall,[921] whether concerning one's body, activities or behavior out in public.

There are indeed legal provisions that mandate technological solutions, but, for the most part, they emphasize only data security. An emphasis on data security is especially not sufficient to address the type of threats posed by the latest PITs. As outlined, many of the latest PITs pose a threat to privacy beyond the consequences of unauthorized access to personal information. The ability to see through clothes or walls, listen and record public conversations, conduct wide-area aerial surveillance, perform brain scans or get into people's heads, and constantly track people's movements are just a few examples of privacy threats that data security nor information privacy alone can nowhere near adequately address. Moreover, given the legal requirements for safeguarding privacy and the different privacy risks, the law must significantly go beyond legal provisions that only mandate technical solutions for data security (Borking, 2010). Therefore, *privacy* by design is what is called for and not just data security by design. Besides, a mere emphasis on data security alone to address privacy threats implies that it is basically always legitimate to collect personal data, as long as it is kept secure.

Where applicable, a holistic approach must be taken, whereby all the privacy principles are incorporated into the design of the system or device concerned. As opposed to only emphasizing on the security of personal data, the technical solutions should, for instance, also control what personal data may be collected or accessed, when and how it may be collected and accessed, for how long it may be stored, and provide data subjects the means to access their stored personal data.

---

921 see Online consultation comments on the European Commission staff paper "Early Challenges to the Internet of Things", Comments submitted by CA, Inc., p. 6, available at: http://ec.europa.eu/information_society/policy/rfid/library/index_en.htm

Without taking into consideration the other principles of privacy, within the design and functionality of the relevant system or device, a diminishing realization or viability of those principles will eventually result. For example, with regards to the access/participation privacy principle, while a data subject's right to request access to the information stored on them by a data controller is provided for within, e.g., Directive 95/46/EC, the implementation of this right will likely be too difficult, impractical or costly, if the relevant system has not been designed or developed in the first place to execute this request efficiently and cost-effectively.

The principles of privacy protection must be built into PITs all at once, where applicable, before their deployment and activation, as opposed to merely bolting them on in a piecemeal, incremental approach sometime after the threat arises. As van Blarkom, G.W. et al., argue "the postponement of dealing with personal data implications 'until a later phase', may easily lead to an information system that is contrary to privacy adaptations" (van Blarkom, G.W. et al., 2003, p. 8). "Certain measures may have been necessary very early on when developing the system before much of this system has been 'cast in stone'" (*Ibid*.). We have already seen the problem with, for example, Google Street View's approach to ensuring privacy by blurring faces and license plates after the images were generated, the service was put online, complaints were made and the damage had already been done. Unsurprisingly, this approach still more than likely leaves tens of thousands of people still potentially identifiable, especially if the ability to zoom in extensively exists. The zoom in capability also allows users to look into people's homes. Instead, a method of ensuring all the privacy principles, where applicable, should have been automatically applied at the moment *when* the images were being generated by the special cameras on Google's Street View vehicles.[922] We have also already seen the consequences of developing the Internet without privacy and security issues fully taken into consideration at the very beginning. Perhaps, if the Internet was designed and developed with privacy/security taken into consideration, some of the significant cyber-security challenges we increasingly face today would have been minimized. As ICT increasingly becomes evermore pervasive, hopefully the ICT industry will not repeat the same mistake with the development and deployment of RFID applications, neurotechnology applications, software agents, intelligent transportation systems and smart electricity distribution grids.

PBD can potentially address almost any threat to privacy at the earliest possible stage of a PIT's lifecycle – i.e. during the research, design and development stages. Accordingly, the built-in technical solutions should be realized before the PIT is deployed

[922] The lack of privacy considerations when developing Google Street View has also likely brought about the fact that Google's Street View vehicles have also reportedly collected data transmitted on private, non-secure Wi-Fi networks.

and in use, rather than addressing the corresponding privacy threat with a hodgepodge of technological band-aids hastily stuck on after the injuries to privacy could occur or have already occurred. In other words, PBD is not about decorating a cactus tree to look like a Christmas tree that will likely prick you anyhow; it is about growing that Christmas tree. As argued in the European Disappearing Computer Privacy Design Guidelines, which forms a part of the 'Ambient Agoras' project coordinated by the Integrated Publication and Information Systems Institute (IPSI) of the German Fraunhofer Gesellschaft (FhG), "[p]rivacy enhancement is better obtained by actively constructing a system exactly tailored to specific goals than by trying to defend ex-post a poor design against misuse or attacks".[923]

However, neither law nor technology alone can ensure privacy is maintained and both are not self-sufficient (Reidenberg, 2000). As Reidenberg (2000) further argues, both *forms of regulation* "embody inherent limitations that preclude adequacy for effective protection of privacy". Therefore, a combination or mixture of law and technology is required to safeguard privacy. PBD is that *critical combination* of law *and* technology.

10.4 NOT A SUBSTITUTE FOR LAW

Indeed, while PBD may significantly ease the dependence of privacy/data protection on user-level regulations and the compliance thereof, legislative instruments or other legal instruments will not simply become obsolete with technological solutions. As Bruce Schneier, a renowned security technologist and author, similarly points out, while technology is key to protecting privacy, in the end, as Schneier emphasizes, privacy boils down to the existence of laws and legal protections.[924] PBD solutions (nor computer code) are not a substitute or replacement for law, but rather are complementary to law. Advocates of PBD do not propose to replace lawmakers with computer programmers or engineers. Similarly, computer code, when used to enforce privacy/data protection laws, does not become law, but remains as the technical means to enforce the laws (see Dommering, 2006). For instance, as Schwartz argues, a technical solution like P3P is necessary to provide the machine-to-machine protocol to enable a web browser and website to negotiate privacy standards, but laws are also necessary to require that those

923 Lahlou, Saadi. and Jegou, Francois. *European Disappearing Computer Privacy Design Guidelines*, Version 1, Ambient Agoras Report D15.4, Disappearing Computer Initiative (Oct. 2003), p. 4.

924 Schneier, Bruce. "Strong Laws, Smart Tech Can Stop Abusive 'Data Reuse'" (Wired News, 28 June 2007), available at: http://www.schneier.com/essay-175.html

negotiations take place (2000, p. 759). Besides, PBD should be based on law (see, e.g., Hildebrandt and Koops, 2010).

As far as possible, technological/design solutions for protecting privacy aim to minimize the intrusive capabilities of the technology concerned and to realize the fundamental principles of privacy. The solutions, however, will often not be able to entirely eliminate the privacy-intrusive capabilities of all PITs, and some solutions will be vulnerable to hackers. Moreover, since certain PITs will need to be intrusive, e.g. for law enforcement purposes/surveillance activities, constitutional and other legal protections will, thus, still need to be significantly relied upon.

Thus, PBD solutions, in the end, are just as important as the laws, rules, regulations, principles and norms that mandate or require these solutions be implemented, influence the end result of PBD, provide the legal control mechanisms to intervene in the chain of production, specify the liability of not complying, punish those who illegally hacked or intentionally circumvented the PBD-based solution, ensure transparency and establish the enforcement and audit mechanisms. There will also certainly still be a need to regulate human behavior or the ways in which PITs are deployed and used. In addition, the law altogether must be capable of ensuring that the inappropriate or unlawful development and use of PITs is not committed with impunity and that there are explicit penalties for violations, available remedies for victims and enforcement mechanisms in place.

Regulating the design and manufacture of PITs alone, therefore, is not enough. Regulations on the deployment and use of body scanners, HIMs and enhanced CCTV capabilities are still required. For this reason, throughout the dissertation, an assortment of different legal proposals was targeted at both the manufacturers/developers of PITs and the operators/users of PITs and/or data controllers.

Yet, the nature and content of these user-level regulations can still depend on the design of the PIT concerned, and vice-versa. For instance, laws that specify when the use of body scanners may be reasonable and according to what level of suspicion, in accordance with the Fourth Amendment, are dependent, for instance, on the final design and specifications of the body scanners, i.e. their level of intrusive capability in the first place.

Even though HIMs and the system thereof can be designed in a way that aims to secure the privacy of the implantee, this does not mean all people should be required to have a HIM implanted or that their implantation should be a condition of exercising other rights. In addition, HIMs, even with integrated PBD solutions, will still collect location information. The law must, therefore, also clarify what are the appropriate circumstances surrounding the use of HIMs and the location information generated by them.

Although CCTV microphones can be designed to only detect and record certain sounds that we all agree are threatening, this does not mean that the law should not regulate what can be done with those recordings afterwards. While developing CCTV loudspeakers in a way that does not permit operators to freely say what they want prevents abuse and reduces the power to disturb and agitate the right to be left alone, the law must still specify where the loudspeakers may be deployed and when their use is justified and/or proportionate to legitimate aims.

10.5 FLEXIBILITY VS. SPECIFICITY

The law, in terms of privacy protection, is often enhanced either with greater specificity through additional specific legislation or additional specific provisions/amendments in existing laws. Specificity helps to allow the law to be predictable and consistent, removing ambiguity, and is also necessary for ensuring enforceability. However, *both* greater precision and clarity and sufficient room for flexibility is needed. Flexibility allows for the adjustment to new circumstances or the emergence of new technologies, which is especially required in a world of constantly advancing PITs. But, where PBD and existing legislation might not provide adequate safeguards for the most privacy-intrusive and disruptive technologies, further specific regulations should also not be overlooked.

Sometimes flexibility in law is effective, while at other times more specificity is required. For instance, the legal definition of personal data and the definitions of what constitute PITs, location information and tracking devices require flexibility, in order to ensure all applicable technologies, devices, etc. are broadly covered now and in the future. On the other hand, the definition of location information also requires a certain level of specificity, in order to cancel any doubts or close any legal loopholes concerning the privacy of location information. Moreover, stipulating where and when location tracking is lawful and stipulating which particular sounds and words, for example, may activate CCTV microphones to begin recording clearly require a certain degree of specificity.

Potential PBD legislation, in particular, also requires flexibility, since it is nearly impossible to delineate every design and technical requirement and also unhelpful to overly prescribe the PBD solutions. The goal indeed, therefore, is for the potential PBD legislation to be as broad and comprehensive as possible when mandating the implementation of PBD solutions. Nevertheless, the PBD solutions will also need to consider the specific characteristics and privacy threats/risks of the different devices, systems or technologies concerned.

10.6 RADICAL CHANGES FOR RADICAL CAPABILITIES

The dissertation research has shown that although body scanners, HIMs and CCTV microphones and CCTV loudspeakers pose a significant threat to privacy and liberty, this threat is not insurmountable. New and enforceable regulations can help to ensure that the development, deployment and use of the latest PITs are regulated adequately.

While the specific legal and technical solutions recommended for body scanners, HIMs and CCTV microphones and CCTV loudspeakers can potentially address the unique threats posed by each PIT, it is, nonetheless, not realistically possible and may indeed be impossible for lawmaking to always keep up with technological developments through *ex-post* lawmaking. It is neither feasible nor ideal to legislate for each and every new technology after it has been deployed or has hit the market or to legislate for every subject matter or domain in terms of privacy protection on a case-by-case basis. This approach will likely continue to result in the adoption of legal solutions that are, for the most part, too little too late and inadequate within years, and vulnerable to the wording and interpretations of the provisions. It is also neither feasible to rely on closing all the relevant legal loopholes or solving all the deficiencies in the law, where applicable, with legal amendments or additional sectoral, technology-dependent laws. Besides, the legal framework in the US, for instance, is already excessively fragmented. Moreover, *ex-post* lawmaking often takes considerable time and, for certain activities and technologies, it may already be too late.[925] New and radical technologies (and corresponding new and radical capabilities) require *new and radical changes to current approaches* for safeguarding privacy.

Although formulating comprehensive, technology-independent data protection/privacy legislation, in the traditional sense, is certainly a great start, such legislation can neither possibly cover all threats to privacy posed by the latest technologies in existence, let alone those yet to be developed or imagined. Essentially, the most comprehensive and far-reaching privacy legislation in the world, Directive 95/46/EC, cannot even address all the present and future threats to privacy, and for that reason the European Commission has proposed a new General Data Protection Regulation to replace Directive 95/46/EC. Moreover, as Reidenberg (2000) points out, enforceability is another limitation on the efficacy of comprehensive legislation, in the traditional sense. While Directive 95/46/EC establishes enforcement mechanisms, global data processing poses significant challenges to their effectiveness (Reidenberg, 2000).

[925] see, e.g., Cave, J., et al. *Trends in connectivity technologies and their socio-economic impacts*, Final report of the study: Policy Options for the Ubiquitous Internet Society, (RAND Europe, July 2009), p. 17.

The RISEPTIS Advisory Report rightfully advocates for ensuring that the development of law is "closely interlinked to technological progress", however, rather erroneously argues in favor of doing so in a reactive manner (2009, p. 31). In order to genuinely stay ahead of the game and to overcome the difficulty of legislating and keeping up with the development of technology, lawmakers need to be proactive and not reactive, looking forward rather than backward, in addressing the implications of PITs beyond tomorrow. Instead of reactively interlinking law with technological progress, in the words of US Secretary of State Hillary Clinton, "we need to synchronize our technological progress with our principles".[926] The law must steer the development of technology, and not the other way around, through *ex-ante* lawmaking, in combination with *ex-post* laws. As Cave et al. (2009) argue "rapid and potentially disruptive technological development and the possibility of profound and irreversible impact upon human characteristics and development call for a careful balance of *ex ante* and *ex post* regulation" (Cave et al., 2009, p. 16). On this basis, legislators can and should 'future-proof' lawmaking pertaining to technology, and should develop *ex-ante* solutions for protecting privacy and ensuring other democratic principles/values that stand a far better chance of being adequate in the long-term and are better equipped for withstanding the test of time.

Going forward, a fresh, one-size-fits-all (legal wise) and technologically neutral/technologically independent legal method is required, as far as possible. The PBD approach to upholding privacy (and other civil liberties) can be potentially applied to just about any PIT and is arguably a feasible solution to the difficulty of keeping up with technology. PBD is a more practical substitute to legislating for each and every new technology, whether already deployed, in the R&D stages or yet to be imagined, that poses a threat to privacy, irrespective of the legal framework.

Although each technology (i.e. PIT) may require specific, individualized PBD solutions in their own right and, therefore, the PBD solutions cannot be technologically neutral, the underlying neutral approach is to require any technology (system, device, service, etc.) to be designed in a way that incorporates all the principles of privacy,

[926] see the prepared text of the speech US Secretary of State Hillary Clinton delivered at the Newseum in Washington DC on the topic of Internet Freedom (21 January, 2010), available at: http://www.state.gov/secretary/rm/2010/01/135519.htm
Similarly, European Commissioner Viviane Redding, formerly of DG Information Society & Media (DG INFSO), and now responsible for DG Justice, Fundamental Rights and Citizenship, stated, during a DG INFSO staff general assembly on 12 February 2010, "although I am not going to be your commissioner anymore, I am going to be still your policy maker". What this means, I think, is that Commissioner Redding believes that ICT research and technological development, an area she was previously responsible for, should be aligned with the principles of justice and fundamental rights, an area she will now be responsible for.

where applicable, through built-in technical and design safeguards. Thus, PBD should be viewed as the core of permanently defending privacy against the threats to privacy and liberty posed by PITs, rather than temporary fixes at the periphery. While there may be some distinctions on how different actors (governed by different laws and needs) may be involved in using the same technology for different purposes, especially in light of creating PBD policies/requirements, the PBD approach is applicable regardless of the technology, legal framework or activity concerned. Overall, the PBD approach, therefore, should be technologically, entity and activity-neutral.

The law should move away from focusing primarily on data controllers and the users/operators of PITs, and should instead impose PBD requirements/obligations on the manufacturers/developers to constrain the privacy-intrusive capabilities of PITs in the first place. Accordingly, new and comprehensive PBD legislation should be adopted, mandating that the principles of privacy must be engineered into all PITs (with certain exceptions) manufactured/developed for private use and/or commercial sale *and* government use in the jurisdiction concerned. On the other hand, once again certain technologies/devices, such as surveillance technologies, strictly used by governments/competent authorities for law enforcement and/or military purposes, for example, may still need to be designed in way that *more* effectively violates privacy, while still complying with the relevant laws and constitutional protections concerning their development, deployment and use. Nevertheless, PBD requirements/obligations should overall still be applicable for technologies developed for law enforcement purposes.[927]

Comprehensive legislation mandating PBD could also potentially refer to ISO standards on data security, as Agre recommends (1997, p. 25), which is known as the "co-regulation model", whereby standardization is used to complement regulations. Alternatively, explicit PBD provisions could instead be further incorporated into existing (privacy/data protection) legislation for different domains and technologies. Moreover, PBD provisions/requirements could also be incorporated into existing legislation on

[927] Importantly, this is consistent with the EC's Proposal for a Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data, COM(2012) 10 final, Brussels, 25.1.2012. Article 19 requires Member States to ensure that data controllers are complying with obligations arising from *data protection by design* and p*rivacy by default*.

defective products and the liability of manufacturers thereof.[928] However, adding some specific provisions to existing legislation may not be sufficient.

Either way, the legal requirements to implement PBD should be applicable, where relevant, to *both* private and public entities and *both* manufacturers/developers of hardware *and* software (i.e. technology providers) and data controllers/service providers.

Accordingly, Article 23 of the official draft EU General Data Protection Regulation,[929] which proposes *data protection by design* (i.e. PBD) requirements, should further stipulate that these requirements also apply to the manufacturers/developers of the products and services in question. The application of Article 23 (paragraphs 1 and 2) to manufacturers/developers could bring greater legal clarity and purpose to paragraph 3 of Article 23, which empowers the EC to adopt delegated acts specifying appropriate technical measures/mechanisms (i.e. PBD solutions) for implementing PBD for products and services.[930] As a result, the draft proposal should also include a definition for "manufacturers" and "developers", in order to diminish any legal ambiguity.

For all practical reasons, however, it will be difficult, for the most part, to apply PBD legislation retroactively, i.e. to existing (or already developed and deployed) devices/products/systems. PITs previously developed and deployed before the enactment of PBD legislation will certainly continue to exist in society and originations, and will thus need to continue to be regulated primarily by user-level and *ex-post* regulations, where applicable. Thus, there will be a period of transition before achieving the new reality and specific objectives PBD promises. To address this limitation, the concept of "*Privacy by ReDesign*" was developed to apply PBD to existing systems by '*rethinking, redesigning* and *reviving*' these existing systems in a way leading to the end goals of PBD.[931] Additional shortfalls, constraints and limitations of the PBD approach are explained in section 10.19.

---

928 Consumer Product Safety Act of 1972; Consumer Product Safety Improvement Act of 2008; Directive 1999/34/EC of the European Parliament and of the Council of 10 May 1999 amending Council Directive 85/374/EEC on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products.

929 see Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11/4 draft.

930 Article 23, para. 3, could potentially have an indirect effect on the manufacturers/ developers, since the specification of appropriate measures/mechanisms for implementing PBD for product and services would likely put pressure on the manufacturers/developers of those services/products to conform.

931 Seminar of the 33rd International Conference of Data Protection and Privacy Commissioners, *Privacy by ReDesign* Workshop, Mexico City, Mexico, November 1, 2011.

Ideally, both the US and EU, and beyond, should adopt PBD legislation, given the global nature of the privacy problems/threats at hand and of the Internet. For instance, PBD legislation in the EU would be pressed to regulate any Google services, for example, that utilize servers based in the US. Nevertheless, even if only the EU initially passes fully-fledged PBD legislation (or incorporates additional PBD requirements into the draft General Data Protection Regulation), for regulating PITs (or initially just ICTs and digital services) manufactured/developed for use and/or sale and/or marketed in the EU, this would also have an impact in the US and on companies that do business in the EU. Furthermore, EU PBD legislation could alter US legislation. For example, REACH, the EU regulation on the safe usage of chemicals,[932] has had an extra-territorial impact on US companies and has influenced US regulations, since entering into force in June 2007.[933] Moreover, the mere existence of PBD legislation in the EU will likely also put pressure on the US Government to pass similar legislation.[934] In any case, as Cannataci points out, EU-compliant ICT/information systems could eventually develop into the *de facto* standard for most devices, infrastructure, systems etc. deployed in the US (Cannataci, 2011, p. 185). But, without common standards, between the US and the EU, interoperability issues will further emerge.

As outlined earlier, codes of conduct, voluntary best practice guidance, guidelines, privacy policies or other self-regulatory schemes are not absolute alternatives to binding law. There is ample evidence to indicate that laws should not and cannot be ditched in favor of industry self-regulations. For example, we have seen the negative consequences of this within the banking sector. Industry self-regulation has also arguably failed to regulate online privacy. Accordingly, while PBD legislation could form the basis of binding corporate rules, PBD requirements cannot and should not be laid down in more voluntary codes of conduct or self-regulations, but rather must be mandated by binding 'hard' laws. Similarly, we should not and cannot rely solely on companies (or government bodies) to always voluntarily comply with self-regulations. Technical

---

932 Regulation (EC) No 1907/2006 of the European Parliament and of the Council of 18 December 2006 concerning the Registration, Evaluation, Authorisation and Restriction of Chemicals (REACH), establishing a European Chemicals Agency, amending Directive 1999/45/EC and repealing Council Regulation (EEC) No 793/93 and Commission Regulation (EC) No 1488/94 as well as Council Directive 76/769/EEC and Commission Directives 91/155/EEC, 93/67/EEC, 93/105/EC and 2000/21/EC

933 see, e.g., Black, Harvey. *Chemical Reaction: The U.S. Response to REACH* (Environmental Health Perspectives 116, March 2008).

934 For further discussion on possible explanations for the convergences in data protection policies/laws between the US and Europe, see Bennett, Colin. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Cornell University Press, 1992).

solutions cost money and avoiding or delaying compliance may be the easy way out. Companies and governments do not enjoy a reputation of always volunteering to absorb these costs or to grasp the additional undertaking in the name of privacy or data security. The confidence of consumers and citizens in governments and particularly in companies, with regards to privacy and data protection, is already far from ideal.[935] While the trust and confidence of consumers and citizens can also partly be achieved through potentially enforceable codes of conduct or self-regulations, hard legislation has the highest positive impact due to the stronger possibility of enforcement.[936] Although codes of conduct, privacy policies, self-regulations, etc. on PBD can be potentially enforced through supervisory authorities with enforcement powers, there are still no guarantees that these industry codes, policies or self-regulations will be adequate or compatible with the fundamental principles of privacy.

Besides, PBD should be implemented through ‘hard’ laws developed by political representatives, since this would be more consistent with the values of a democratic society, which require that “rule-making through technology must be shaped by public policy goals and debate” (Reidenberg, 2000). Therefore, if computer code can have the same, if not greater, effect in practice, then technological development must be brought into democratic processes.

10.7 IMPLEMENTATION, ENFORCEMENT, MONITORING AND EVALUATION

In line with the typical phases in policymaking/lawmaking, once PBD legislation and policies are put in place and the measurable and feasible objectives/targets are fully formulated and established, the legislation must then be gradually implemented and enforced accordingly, subsequently monitored and, after a certain period of time, evaluated on its effectiveness. Perhaps, a High Level Working Group (composed of mem-

935 Though consumers’/citizens’ trust in public institutions to handle their personal data appropriately and their level of confidence in privacy policies is not perfect, according to a Eurobarometer survey in 2008, more than a majority of EU citizens do have this trust and confidence in different types of public institutions. However, considerably less than a majority of EU citizens have this trust and confidence in companies, such as credit card companies, travel companies, market research companies and mail order companies. see Flash Eurobarometer Series #225, Data Protection in the European Union - *Citizens’ Perceptions* Survey, conducted by the Gallup Organization Hungary upon the request of the Directorate-General Justice, Freedom and Security of the European Commission, Analytical Report, February 2008.

936 see Commission Staff Working Document, Impact Assessment, Accompanying document to the Commission Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification “RFID Privacy, Data Protection and Security Recommendation” {C(2009) 3200 final}

bers from different public authorities and various stakeholder representatives) could be established to monitor, oversee and guide the initially complicated implementation/enforcement of the PBD legislation.

The diagram below outlines the implementation/enforcement steps for PBD legislation, including the main causes and effects, some of the preliminary indicators for measuring the enforcement, effectiveness and realization of the policy objectives/targets, and the links with other relevant key policy instruments/laws in the US and UK that serve as its basis.

The implementation/enforcement mechanisms, consisting of certification bodies, privacy audits, conformity declarations, recalls and sanctions, are briefly explained further in the following sections.

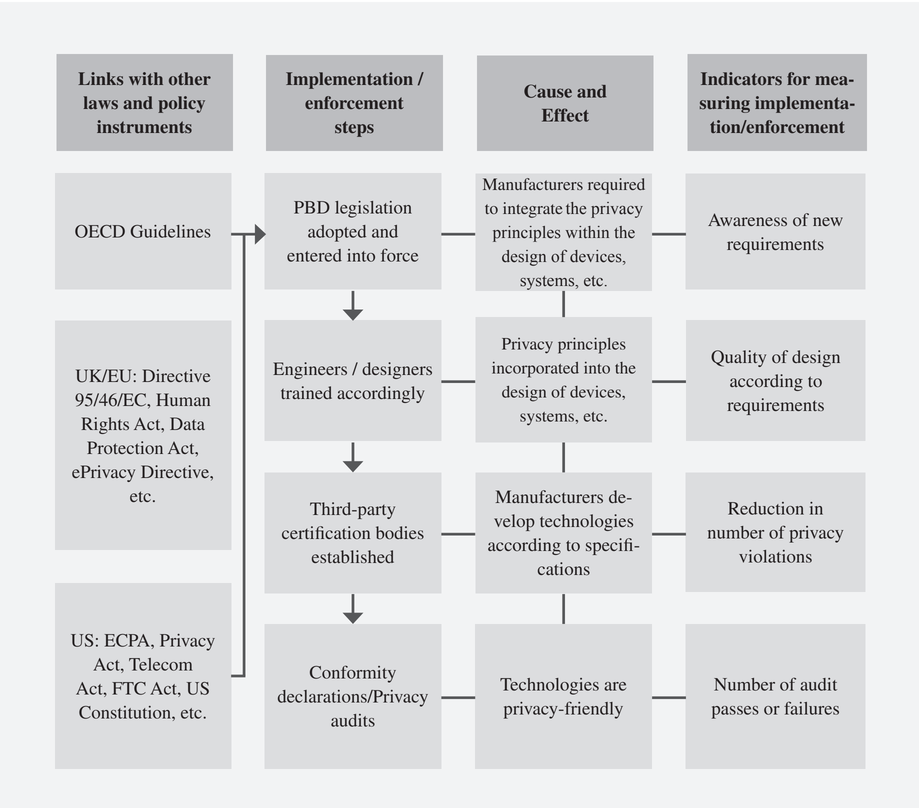

Figure 4: PBD implementation/enforcement

After a certain period of time, e.g., 3-5 years, a review process should be externally commissioned to evaluate/assess the status of the implementation/enforcement and the effectiveness of the PBD legislation, in order to determine if any adjustments and/or further policy measures/instruments are needed.

The overall long-term responsibility for monitoring the implementation/enforcement of the PBD legislation should reside with governmental data protection/privacy supervisory authorities.

10.8 ACCOUNTABILITY, SANCTIONS AND RECALLS

Manufacturers/developers (i.e. technology providers), in particular, should be held accountable/liable for failing to incorporate adequate and verifiable PBD solutions/technical measures that do not include both privacy and security functions, where required and applicable.[937] Likewise, manufacturers/developers should be held accountable/liable, under a similar liability structure, for 'privacy defective' devices/products *and* services that result from demonstrated negligence/fault and cause significant damages to a person as a consequence.[938]

The legal accountability of the manufactures/developers can come through the application of sanctions and product recalls, where deemed necessary. Sanctions could be imposed on the responsible manufacturers/developers and the individuals substantially affected may also be entitled to receive compensation.

In addition, where and when privacy/security failures emerge or non-compliance is discovered after the fact, whether intentionally or unintentionally, if the effects of the failure or non-compliance pose threats or risks to privacy and/or data security deemed to be serious, a recall of that product, device, etc. should also be enacted. A company's desire to prevent or avoid the risk of needing to initiate a recall of their products, devices, etc. could provide the necessary incentives to fulfill their obligations.

In the absence of an applicable manufacturer/developer within the concerned legal jurisdiction, then the designated official importer could also be potentially held respon-

---

937 For instance, Senator Patrick Leahy previously introduced S.1490, entitled "the Personal Data Privacy and Security Act of 2009", which aims to hold software companies liable for security flaws or vulnerabilities and mandates that business entities implement data privacy and security technical and physical safeguards in the system's design and imposes civil penalties on entities that fail to do so. While the legislation essentially covers 'information privacy', as opposed to the protection of privacy overall, this proposal has some similarities to the proposed PBD legislation.

938 A perfect example of a privacy defective device/service includes certain models of the Trendnet home security cameras that were discovered to have flawed firmware allowing anyone to access online live feed without requiring a password.

sible for publicly declaring that the device, product, etc. complies with the relevant PBD requirements/laws.

Nevertheless, the liability of manufacturers/developers should be subject to certain exemptions. For starters, manufacturers/developers should not be held liable for the unlawful use and/or modification of their products/services, whether by government or other private entities. Furthermore, under certain exceptions, if manufacturers/developers can prove that the privacy violations are not the direct result of inadequate PBD solutions or the lack thereof, they may also be exempted from liability. Finally, the so-called "state of the art defense"[939] should also exempt manufactures/developers from liability.

10.9 CERTIFIED PRIVACY-FRIENDLY

While privacy protection cannot necessarily be measured or quantified in the normal or traditional sense, a privacy compliance audit of the design of the PIT concerned could be conducted after the technical and/or architectural design solutions are built-in. The audit could serve to re-examine any residue privacy threats/risks and to determine or verify the quality and adequacy of the solutions in meeting certain objectives and complying with the principles of privacy and relevant laws.

Serving as a quality assurance mechanism for PBD, a privacy certification scheme may be effective in verifying that a PIT has been designed adequately in terms of privacy protection and incorporates adequate technical solutions. However, the principles of privacy provide the goals that need to be met with PBD, but do not actually provide the methodologies for achieving these goals, nor for evaluating the adequacy of the end result of PBD. The certification scheme will, thus, require its own evaluation criteria and measurement techniques for determining the validity and adequacy of the PBD solutions for the devices, systems and services concerned.

The certification scheme for PBD, however, should equally not only be based on a voluntary self-certification/self-declaration scheme, such as the 'Safe Harbor' scheme in the US. Instead, the scheme should be independent, external, mandatory and managed/supervised by either a quasi-governmental or governmental certification body, preferably in conjunction with accredited private certification bodies, but not by pri-

939 For example, Article 7 of the EU Directive 1999/34/EC explains the "state of the art defense" exemption. Manufactures can be exempted from liability, if they can prove "t*hat the state of scientific and technical knowledge at the time when the product was put into circulation was not such as to enable the defect to be discovered.*"

vate entities alone.[940] The privacy certification scheme should apply to just about any system, device or service capable of posing a threat to the right to privacy, and not just ICT devices or IT-based/digital services. The accredited certification bodies should be composed of privacy auditors qualified to verify that any device or system has the appropriate built-in safeguards, design/architectural features and technical specifications, based on the principles of privacy and compliant with the relevant laws, and that these safeguards, features and specifications are not easy to bypass.

But, as a first step, developers/manufacturers could potentially or initially avoid external intervention by signing binding 'declarations of conformity'. If subsequently determined to be additionally required, external privacy auditors could conduct an evaluation of the devices, systems or services in question. In addition, random checks/audits could also be carried out.

PITs or any other technology, device or system either presumed or verified to have the required/appropriate built-in safeguards, design features and technical specifications could be certified 'privacy safe', 'privacy-compliant' or 'privacy-friendly' and could be marked with a standard privacy logo or seal.[941] In Europe, for example, the certification scheme EuroPriSe, initiated by the data protection authority of Germany and funded by the EC, has already adopted a 'European Privacy Seal', which is used to reveal to consumers that an IT product or IT-based service has been certified privacy safe and complies with the applicable EU data protection rules/principles. Other privacy seals include the Carnegie Mellon Usable Privacy & Security Lab's so-called "nutrition label for privacy". As the Article 29 Working Party points out, "[a]s certain seals become known for their rigorous testing, data controllers are likely to favour them insofar as they would give more compliance 'comfort' in addition to offering a competitive advantage".[942] An additional way of communicating the degree of privacy-friendliness of a device, technology or system could include the use of "privacy scores", based on the results of the PBD certification audit, similar to the "privacy scores" developed by PrivacyChoice for websites.[943]

Any privacy certification scheme, however, is only complementary to PIAs and should not be considered as the same thing. PIAs, for instance, are intended to be conducted *before and/or during* the development of the technology (or service) concerned,

---

940 A similar approach is used in the EU for the certification of organic products.

941 A similar approach is used in the EU for implementing 'ecodesign' requirements for energy-using appliances.

942 Article 29 Data Protection Working Party, WP 173, Opinion 3/2010 on the principle of accountability, Adopted on 13 July 2010, p. 17.

943 see http://www.privacyscore.com

in order to assess the potential threats to privacy posed by that technology. Moreover, as Cannataci points out, PIAs could induce the implementation of technical measures to safeguard privacy (2011, p. 182) and, therefore, PIAs can still play an important role.

Privacy certification audits, on the other hand, are conducted, for the most part, *after* the technology has been developed with the relevant laws and privacy principles systematically taken into consideration during the research, design and development/manufacturing phases. Thus, before the development stage, the developers/designers, together with privacy experts, will first need to carry out a PIA to carefully identify all the foreseeable privacy threats and vulnerabilities of the device, system or service, as far as possible, and assess the potential risks involved and set benchmarks for removing/minimizing these threats/risks.

Furthermore, while there are established industry standards, implementing measures and audit mechanisms for ensuring data security, and, on top of that, comprehensive guidelines/checklists for conducting general and specific PIAs,[944] additional standards, methodologies, indicators and mechanisms for auditing the adequacy, performance and quality of PBD still need to be established, which embody all the principles of privacy, where applicable, in an integrated approach. ISO has so far at least set up a working group to establish a standard for "privacy technologies".[945] The EC has also called for the introduction of a "European certification scheme for "privacy-aware" technologies, products and services".[946] As the European Organisation for Security (EOS) recommends, the criteria for assessing/evaluating the adequacy of PBD solutions should equally be clear and precise.[947]

944 see, e.g., the ICO PIA Handbook for guidelines on conducting PIAs, available at: http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html;
Privacy and Data Protection Impact Assessment Framework for RFID Applications, 12 January 2011, available at: http://ec.europa.eu/information_society/policy/rfid/documents/infso-2011-00068.pdf

945 see JTC 1/SC 27/WG 5: Identity management and privacy technologies

946 COM(2009) 262 final, Communication from the Commission to the European Parliament and the Council - An area of freedom, security and justice serving the citizen.

947 see Pasic, Aljosa. "Privacy by Design: An industry perspective on the challenges and opportunities of privacy", available at: http://www.eurescom.eu/?id=531

10.10 DESIGNING FOR PRIVACY

It is now increasingly understood that, in order for citizens to enjoy adequate protection of privacy, in light of the digital age, the rapid advancement of technology and the challenges facing existing laws, manufactures/developers need to implement PBD solutions. This should not come as a surprise too many. Designing for an outcome is essential in just about all things. For example, if you want speed, safety and fuel efficiency in a car or airplane, then you must apply the principles of aerodynamics and safety during the design stages, which are then tried and tested. Moreover, if you want productivity and eco-friendliness, then you must design for it. The same concept and approach should possibly apply to privacy protection.

However, while the benefits of PBD are imaginable, it should also be noted, once again, that there is currently no widely accepted methodology or approach for specifically translating privacy/data protection laws into technological/design solutions and there are no accepted standards for auditing the adequacy and quality of PBD. However, valuable research has been conducted to progressively formulate a process. In general, a plausible process is to first analyze the legal framework to determine the required human behavior and then implement those requirements through technological/design solutions (van Blarkom, G.W. et al., 2003). After the PBD solutions are executed or physically realized, a privacy audit is subsequently conducted to determine if those requirements are fulfilled. Nonetheless, even though a common process is helpful, no single fixed methodology or approach is required, or even desirable, as PBD solutions should be somewhat tailored to the specific PIT concerned and, once again, should not be overprescribed.

Since the degree of privacy reasonably expected from the use of PITs is relevant to the degree of privacy the design of those PITs affords, inadequate and poor quality design specifications will only negatively affect or lower our reasonable expectation of privacy. Take, for example, a bathroom stall or changing room door. Clearly, existing privacy laws cover privacy in a bathroom stall or changing room and prohibit the spying or unauthorized observation of a person inside one. But, that prohibition is only as good as the design of the bathroom stall's or changing room's door. If the doors are below 5 feet (1.5 m), for example, or made of see through glass, then by simply walking past them, a person can easily and unintentionally see over the doors or right through them. Hence, any degree of privacy would be non-existent or unreasonably expected in these bathroom stalls or changing rooms simply because of the design of the doors, regardless whether the law clearly stipulates privacy in a bathroom or changing room.

In addition, any technological solution or architectural design for the sake of privacy must seek to transcend time, and therefore designers must attempt to anticipate, as much as possible, the threats to privacy and other civil liberties posed by the technology (device, system, etc.) in question. As Sollie and Düwell (2009) wisely point out, an anticipatory outlook is required when addressing new technologies. The ultimate goal is to develop technological solutions and/or architectural designs that are 'future-proof' for the longest period of time possible to counter-balance the difficulty of 'future-proofing' *purely* legal solutions.

However, while the purpose of PBD is to effectively safeguard privacy and put into practice the principles of privacy, it must also not hinder or terminate the desired purpose, effectiveness and utility of the device, product or service concerned, thereby rendering it useless or ineffectual. Again, the right balance needs to be struck. Designing for privacy should also take into consideration the effects of over-engineering, which can cause a device or system to be more complicated than necessary and decrease its effectiveness and efficiency.

Although the law preferably need not overly prescribe what PBD solutions need to be adopted and implemented, what is essential is that those solutions are goal-orientated, adequate and focused on the minimum expected outcomes. As a final point, when it comes to designing for privacy, some common sense would also do some good. Consider, as an example, the previously explained analogy regarding bathroom stall/changing room doors.

10.11 ADEQUATE PRIVACY BY DESIGN

On the surface, the PBD solutions are adequate as long as they uphold all the privacy principles, where applicable, implement the relevant regulations, and ensure the minimum expected outcomes. The technical solutions, as much as possible, must also not be capable of being bypassed and must be up-to-date and relative/proportionate to the privacy threat at hand.

When determining adequacy, we should assess the extent to which the PBD solutions suitably match the threats to privacy, and the consequences thereof, posed by the technology concerned, evaluate the probability of the pertinent threats still occurring even after the PBD solutions are implemented, and assess the sensitivity of the personal data that may be processed. Hence, this is the reason why an assessment of the privacy threats/risks posed by the technology concerned (i.e. a PIA) must be conducted *before* and/or *during* the technological design/development.

In addition, the technical solutions should also take into consideration the implementation of other civil liberties, where applicable, and not just the right to privacy.

10.12 OVERREGULATION

Specific technical solutions were recommended for each of the four PITs addressed. But, the law should not overly prescribe these solutions, in order to prevent the drawbacks of overregulation. While the law should firmly mandate that public and private entities take the necessary steps to implement technical solutions when designing and developing PITs, it would be advisable for lawmakers not to get involved in determining and mandating exactly which are those solutions, and let the responsible industry players and other stakeholders work that out. But, in any case, those solutions must strictly be based on the defined privacy principles, norms and legal framework.

There are not necessarily single fixed solutions that work for all PITs all the time. Each PIT might require different solutions, based, once again, on the specific characteristics and privacy threats/risks of the technology concerned, and these solutions will also need to evolve as the technology evolves. Moreover, one-size-fits-all PBD solutions could create resistance to innovative and more effective solutions. In this regard, privacy law and the approaches to PBD could learn extensively from environmental law/regulation and the approaches to 'green by design'.

As Hirsch notably argues, 'command-and-control regulation' applied in environmental law, is not necessarily suitable for protecting privacy (2006, p. 33). In environmental law, "regulators identify the best currently existing technology for controlling pollution in that industry (known as the "reference technology")" and "either direct all facilities in the industry to install the chosen technology (this is known as a "design standard")" or require that the facilities do not exceed the rate of pollution they would emit if they had used the reference technology (this is known as a "rate-based standard") (Hirsch, 2006, p. 33).

As Hirsch (2006) further points out, with regards to environmental protection, "command-and-control also deters innovation in pollution prevention and locks in the current state of pollution control technology" (Hirsch, 2006, p.35). The same may hold true, as Hirsch (2006) argues, for privacy protection technologies.

While the "rate-based standard" may make somewhat more sense for protecting privacy than the "design standard", since it may permit different methods or means for achieving the same goal, the "rate-based standard" still relies, in effect, on the reference technologies on which the rate is based, as Hirsch points out, and "almost all [companies] choose the reference technologies so as to avoid any misunderstanding about compliance" (Hirsch, 2006, p. 34). As Hirsch further argues, "[b]y requiring firms to meet the best existing level of control technology, it gives them no incentive to exceed this level" and "the method is too slow for rapidly evolving industries" (2006, p. 35). Therefore, as Hirsch (2006) argues, both standards are just different types of command-and-control regulation and, as a result, both would likely not hold up against the rapidly evolving technological means of privacy intrusion.

The EDPS recommends that PBD could potentially adopt the ‘Best Available Techniques’ (BATs)[948] approach.[949] However, BATs, which are also based on command-and-control regulations, can impel companies to adopt technologies that are already available (Hirsch, 2006, p. 35), thereby diminishing the outlook for developing more innovative technologies that are not yet available.

Moreover, overprescribing the technical/PBD solutions to address the privacy threats of PITs could discourage the continuous development or enhancement of new solutions that could progressively achieve even better results. Unlike the EC’s draft General Data Protection Regulation, which gives the EC authority to mandate specific technical measures/solutions and standards, the proposed PBD legislation, as the US Department of Commerce similarly argues,[950] should instead focus on ensuring the realization and implementation of the principles of privacy as a *policy objective* or outcome.[951] If privacy laws are too prescriptive, as Hirsch also argues, they could stifle technological innovation for protecting privacy (2006, p. 36). Similarly, as the US Department of Commerce also points out, “by requiring a particular technology, a regulator may preclude the implementation of better privacy solutions and stifle innovation that benefits consumers and the economy”.[952]

---

948 The term BAT (Best Available Technique or Best Available Technology) is another example of a concept that was first developed in the context of environmental protection, but its extension into other fields may be appropriate and constructive. Council Directive 96/61/EC of 24 September 1996 concerning integrated pollution prevention and control defines BATs as “the most effective and advanced stage in the development of activities and their methods of operation which indicate the practical suitability of particular techniques for providing in principle the basis for emission limit values designed to prevent and, where that is not practicable, generally to reduce emissions and the impact on the environment as a whole” (Art. 2.11). Techniques include the use of technology.

949 see European Data Protection Supervisor Opinion on the Communication from the Commission on an Action Plan for the Deployment of Intelligent Transport Systems in Europe and the accompanying Proposal for a Directive of the European Parliament and of the Council laying down the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other transport modes, 22 July 2009, available at: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2009/09-07-22_Intelligent_Transport_Systems_EN.pdf

950 see US Department of Commerce, Informal Comment on the Draft General Data Protection Regulation and Draft Directive on Data Protection in Law Enforcement Investigations (16 January, 2012).

951 *Ibid*.

952 *Ibid*.

Likewise, "[e]nhanced privacy protection will depend on the development of new technologies" (Hirsch, 2006, p. 36) and the success of PBD is equally dependent on the availability of the technology to bring about that success. The PBD method or approach to protecting privacy, therefore, benefits from the further development of technology and, as Hirsch emphasizes, "[t]his development requires regulatory methods that encourage innovation, not those that constrain it" (*Ibid*., p. 36). Furthermore, as the US Department of Commerce points out in response to the EC's draft General Data Protection Regulation, "granting the [European] Commission the power to specify technical mechanisms may have the significant unintended consequences because technology developments outpace government regulation".[953]

Instead, the decisions on the specific technical measures/solutions and standards should be left open to a multi-stakeholder process.[954] Companies and other entities should also be allowed to collectively and/or individually select and develop their own method, as long as the selected method is strictly based on the defined fundamental privacy principles and applicable laws. In addition, PBD could also potentially benefit from open technical standards and open collaboration/open innovation.

The smart implementation of privacy protection measures will, thus, require smart regulations. If written smartly, regulations need not slow or halt the innovation of even better technical solutions for the benefit of privacy. Accordingly, PBD, and the privacy laws thereof, should adopt the next-generation regulatory approach, as opposed to an overly prescriptive command-and-control approach (Hirsch, 2006). Next-generation standards, such as Porter's performance-based standards for promoting innovation in environmental protection (see Porter and van der Linde, 1995), which move away from both design standards and rate-based standards, are not based on reference technologies and may, therefore, potentially help to promote the innovation of PBD solutions for protecting privacy by encouraging companies to select/develop their own methods (see Hirsch, 2006, pp. 38-40). The Environmental Management Systems (EMS) may also offer a helpful model for the protection of privacy and the implementation process of PBD, as argued by Hirsch, since EMS often entails continuous improvement practices (2006, pp. 60-63).

---

953 *Ibid.*

954 *Ibid*.

10.13 FURTHERING DEPLOYMENT AND INNOVATION

Some might raise the argument that *ex-ante* regulations on technological development could jeopardize or stifle innovation (Cave et al., 2009, p. 17) or hamper technology deployment and, therefore, could, in the long-run, also impede economic growth and competitiveness (*Ibid.*). Similarly, some might argue that regulating the development of RFID and GPS applications, body scanners, and enhanced CCTV capabilities, among other technologies that are also in their initial phase, will present barriers to their deployment and further advancement. The same argument often supports developing the technology first and asking questions and adopting guidelines later, and maybe, just maybe, if there is no other choice, and as the last resort, adopting relevant regulations only after a serious problem or incident arises.

While the ability to innovate without permission should not be compromised, there is a need for re-adjustment. Instead of applying resistance to the inertia of technological development, a more 'guided hand' approach is needed for steering technological development along a path that does not contradict privacy and other civil liberties and democratic values. This could move us away from the laissez-faire or "invisible hand" approach that has resulted in today's current situation, particularly in the US, surrounding the unrestrained development of PITs, as it has also, to a certain extent, arguably resulted in the ongoing banking/financial industry crisis.

On the contrary, the hurdles to the substantial further deployment, innovation and mainstream take-up of GPS and RFID applications, including location-based services, for example, are partly due to the general perceptions, mistrust and concerns of the public, privacy activists and civil society as a result of the grave threats to privacy posed by these latest technologies and the disbelief in the adequacy of the legal framework to defend against the corresponding privacy threats/risks.

The societal acceptance of the latest technologies is partly interlinked with the public's trust that privacy is respected, and the societal acceptance is often a prerequisite for the deployment and use of the latest technologies. The further development, deployment and use of the latest ICTs is now arguably being held back, to a certain extent, due to the opposition of consumer protection organizations, the lack of trust among consumers/citizens concerning the privacy/data protection issues and the hesitation of manufactures. This hesitation is likely due to these uncertainties and the resulting investment risks. And, once again, the lack of trust can also potentially lead to missed business opportunities and stalled innovation (Williams, 2009, p. 78).

RFID technology, in particular RFID implants, is a perfect case in point. If technologies or devices, such as RFID implants, are to succeed in achieving mass market take-up, the appropriate legal framework and technological architecture is certainly required to earn the critical trust of consumers/citizens. The anxieties of consumers/citizens can potentially be overcome with not just public relations, which aim to persuade the public of the benefits of adopting certain technologies, but also with an adequate legal framework and the appropriate privacy safeguards. Actions often speak louder than words. Moreover, as a result of these perceptions, anxieties and legal deficiencies, manufacturers and service providers are faced with ensuing uncertainties, which could be seriously holding back the mass deployment and further innovation of RFID applications.

Lawmakers can alleviate the resistance and backlash to new technologies and facilitate their roll out and mass market take-up through the adoption of an appropriate and predictable legal framework. Citizens/consumers can be afforded with sufficient safeguards and rights, and developers/manufacturers, data controllers or service providers with clear rules to follow. Specific and up-to-date regulations and PBD solutions will enable companies and governments to earn the long-lasting trust and confidence of consumers/citizens over the use of PITs, thereby facilitating their widespread deployment and use, which in turn could further promote the necessary investments in innovation. Without specific and up-to-date regulations and safeguards, credit cards, for example, would not be able to flourish or function and e-commerce would not be what it is today, as consumers would not have had the required trust in these products or services when they were first launched.

Specific legal regulations on the design, development and manufacture of PITs could also enable the developers to design and manufacture them without concerns or uncertainties over the future legality and liability of their investment. Without specific regulations, the developers have no definitive standards to follow. In addition, the absence of specific regulations could further stifle innovation and lead to uncertainties and confusion for both industry players and consumers alike. As the RISEPTIS Advisory Board also points out, with regards to e-services, appropriate technical and legal infrastructures will remove barriers to innovation, as businesses will only invest in e-service solutions if the legal obligations are clear (RISEPTIS Report, 2009, p. 14).

Moreover, some PBD solutions or concepts could perhaps be innovative in themselves and could lead to further innovation in other related or even unrelated areas. For example, the innovative technology behind Brijot’s ‘intelligent detection engines’ or L-3’s automatic threat recognition (ATR) capabilities for body scanners, developed to better ensure both the privacy and security of air travelers, could also potentially have additional applications and/or could open up additional business opportunities.

Therefore, in addition to protecting privacy, PBD could potentially overall play an essential role in establishing a legal environment that facilitates greater investment in new technologies and, as a result, further innovation, by sending a clear signal to manufacturers/developers on how to move forward with certainty, backed by the confidence, trust and acceptance of consumers/citizens.

10.14 SAFEGUARDING PRIVACY, LIBERTY AND SECURITY

Numerous technologies/infrastructures, which have already been deployed (e.g. body scanners, UAVs, sensor networks, data centers, CCTV cameras, GPS tracking devices, etc.), clearly pose a threat to privacy/liberty. But, these technologies also offer security gains that cannot be ignored, and their deployment may be justified in many respects.

However, protecting privacy and maintaining national/public security is not necessarily a zero-sum game and a choice does not need to be made between protecting privacy and maintaining security (Cavoukian, 2009). Just like there are strong arguments in favor of achieving economic growth in an environmentally-friendly manner, national/public security can evidently also be maintained in a privacy-friendly manner.

Similarly, complying with laws, ethical values or norms does not necessarily cancel the security utility of technologies. Even the most morally questionable technologies can be designed to be 'value sensitive', while still maintaining their effectiveness. For example, missiles/bombs designed in a 'value sensitive' manner, in order to enable military leaders to better comply with the Geneva Conventions, certainly does not cancel their ability to destroy targets. Bombs/missiles are designed and manufactured to kill enemy combatants on the opposing side during a war or to cause immense destruction to the enemy's infrastructure (evidently in the name of security). For a long time, bombs/missiles were designed and manufactured to kill indiscriminately and were not designed to ensure attack precision. That ability to ensure precision was not available. Today, bombs/missiles are still developed to kill and cause destruction. But, at least now most bombs/missiles dropped or launched by the US, for example, during a military operation, are designed to strike a target with precision using GPS guidance, while minimizing the destruction of civilian infrastructure and lives. These bombs are commonly known as "smart bombs". This approach has proved to not only better comply with international laws of war and with overall human values; it has proved to be more beneficial for achieving certain military objectives.

The idea is that we do not always need to think in terms of privacy/liberty vs. security. In fact, in many ways, privacy/liberty vs. security is an increasingly false dichotomy, and we can achieve both at the same time. Especially, through PBD and certain choices of architectures used, the trade-off argument between privacy/liberty and security is less and less valid (Cavoukian, 2009). Privacy/liberty does not need to be sacrificed and we can implement certain boundaries, without losing the security benefits or utility of PITs. There are clear technological examples demonstrating this to be true.

As deducted from the case studies, designing and developing body scanners, HIMs and CCTV microphones and loudspeakers, along with other PITs, in a privacy-friendly manner, in order to better comply with privacy laws and principles, not only does not cancel the national/public security benefits these PITs can provide, the proposed PBD solutions can potentially help to better realize or amplify those benefits.

The automatic employment of privacy algorithms/software solutions when body scanner images are generated, together with intelligent detection engines or ATR capabilities, can (potentially) help airport screeners/security officers to detect/locate threats by highlighting objects and reducing human errors. At the same time, these measures better protect the privacy of the human body (passengers) by reducing the unnecessary level of graphic detail contained in the images and/or potentially doing away with the need for remote human operators to directly view the images. Built-in limitations on storing, printing and transmitting the body scanner images can also better ensure the privacy principles are implemented. Regulating the design and manufacture of body scanners, and thereby limiting their intrusive capability, will arguably lead to their greater deployment and employment at airports (and maybe at other areas/locations on a case-by-case basis, e.g. train stations or major sports stadiums), which may be beneficial for security overall.

Strong encryption in RFID implants, which prevents ‘cloning’ and the unauthorized access to the information contained on the implants, and protocol-level controls, which can ensure that only authorized readers are able to read RFID implants, also allows for the security benefits of electronic identification and tracking to be realized, where and when appropriate.

Designing and developing CCTV microphones to pick up only on dangerous sounds, such as gun shots, explosions and breaking glass, allows the microphones to only focus on the sounds and scenes worthy of being detected and recorded, and deserving of the immediate attention of CCTV operators. The potential sound detection capability of microphones attached to CCTV cameras can enhance the ability of the cameras and CCTV operators to aid in criminal investigations and support public security, remove the blind spots of CCTV cameras and reduce the number of cameras needed to cover a larger area, while at the same time can facilitate a certain level of privacy out in public and minimize the unnecessary intrusion upon the public interactions of citizens. Moreover, this system can more effectively and efficiently employ/deploy CCTV control room operators for the sake public security.

Designing and developing CCTV loudspeakers in a way that enables their use to be registered and prevents abuse, for instance, also allows the operators to accurately document and analyze where and how the loudspeakers can be more effectively used and deployed.

Therefore, PBD can provide potentially effective means for avoiding the (false) dichotomy of *privacy vs. security* (Cavoukian, 2009)[955] and, for that reason; PBD may be a pragmatic and integrated approach for safeguarding privacy, liberty and security in the 21st Century.

10.15 PRIVACY-FRIENDLY ALTERNATIVES

Even though body scanners, HIMs and enhanced surveillance capabilities may arguably be the most effective in preserving security in their respective field or domain, and the threats to privacy they pose can be minimized, there may be alternative devices or means available that are more privacy-friendly (or privacy-compliant), but arguably also provide similar benefits. Many of these alternatives were described in the previous chapters, and some should be further explored in future studies to definitively determine their pros and cons in more detail.

In any case, the least privacy-invasive technology overall should be used, in accordance with the principle of proportionality, as long as it is capable of providing similar benefits, for example, in terms of security. If the more privacy-friendly alternative is not used, the legal and factual reasons for not doing so should be justified accordingly.

10.16 COUNTERING POTENTIAL CRITICISM OF PBD

In response to potential criticism (see section 9.11), PBD does not rely excessively on individual "privacy control". Indeed, PBD is an answer to Schwartz's (2000) criticism of "code as law", since PBD can serve as the means of *automatically* realizing the principles of privacy. In other words, PBD aims to implement the mandatory and default rules/principles of privacy protection primarily in a self-executing manner, i.e. without the constant involvement of individual choice or human intervention.

Moreover, while politics and market dynamics should obviously not be ignored, the effectiveness of PBD is not overly contingent on finding the "optimal mix" of the different modalities/dimensions of regulating technology development. Indeed, one of the main reasons for mandating PBD is to overcome current market failures and, above

---

[955] see also Ann Cavoukian's "7 Foundational Principles of *Privacy by Design*", Originally Published: August 2009, Revised: January 2011, available at: http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

all, PBD is about the implementation of privacy laws/principles primarily through technological/design solutions.

The PBD approach is also compatible with the way lawmakers, legal practitioners and courts operate in the real world. After all, the concept behind PBD already has a legal basis in the US and EU, and the EC's draft proposal for a General Data Protection Regulation proposes PBD requirements. While the current (and proposed) privacy/data protection laws *primarily* apply to data controllers/processors, and not technology developers/manufacturers, there is, nevertheless, also a legal basis for this approach. Patient safety, automobile safety and consumer and environmental protection laws, for instance, already regulate how certain products are designed and developed/manufactured.

Given that PBD will require traditional legal approaches and is not a substitute for law or lawmakers, but is rather meant to enforce existing laws, norms and principles (see section 10.4); there is also little or no reason to assume it is incompatible with democracy. As Schwartz similarly argues, the application of the privacy principles (or FIPs) ensures the involvement of our democratic institutions, and since PBD is based on the principles of privacy, lawmakers are already involved in the process of shaping the technological requirements and solutions (Schwartz, 2000, p. 787).

Furthermore, Grimmelmann's warranted analysis that computer code/software is also *malleable* and *vulnerable*, and is not the same as physical architecture,[956] is offset by the fact that PBD includes *both* physical design/architectural solutions and technological/software solutions. PBD does not aim to equate the two types of solutions.

10.17 OVERCOMING SOME OF THE CHALLENGES

First of all, in order to ensure that the necessary PBD solutions can be developed appropriately, the underlying PBD requirements mandated through PBD legislation will need to be clarified precisely and consistently.[957]

Furthermore, as the European Organisation for Security (EOS) also proposes, research-funding programmes should fund studies that aim to identify and address the needs for the development of concrete, specific and viable PBD solutions.[958] In line with these views, the European Commission (Trust & Security unit) plans to fund, un-

956 Grimmelmann, James. *Regulation by Software* (Yale Law Journal, Volume 114, 2005), pp. 1719-58.

957 For further discussion, see Pasic, Aljosa. "Privacy by Design: An industry perspective on the challenges and opportunities of privacy", available at: http://www.eurescom.eu/?id=531

958 *Ibid*.

der the Seventh Framework Programme (the EU's main research-funding programme), projects that aim to facilitate the interplay between various stakeholders and actors, in order to preliminarily establish best practices, standards and a roadmap for promoting and implementing PBD.[959]

Companies, researchers and other stakeholders could also receive public funding to develop and validate a variety of PBD solutions, and then identify and exchange best practices and lessons learned for implementing PBD solutions, based on established facts/evidence and pilot demonstrations. This could also help to provide the required inspiration, driving force and knowledge/evidence for developing/adopting PBD legislation and for developing a sort of checklist for PBD procedures. Subsequently, public funding could also be made available to establish dedicated PBD training programs for computer programmers/engineers and to communicate the identified best practices and lessons learned.

In addition, a rewarding scheme for the best PBD solutions could stimulate excellence in PBD and the engagement of highly qualified and creative designers and engineers. Adding PBD as a category to the International Design Excellence Awards (IDEA), for example, could help to stimulate the required excellence in PBD.

10.18 ENGAGING RELEVANT STAKEHOLDERS AND OTHER ACTORS

The success of PBD will also require the engagement, inter-communication and information/best practice exchange between a variety of relevant stakeholders and actors, from the manufacturers of PITs, and their engineers, programmers and designers, to lawmakers, regulators, policymakers, privacy commissioners, privacy officers, lawyers, certification bodies, certified PBD trainers, privacy certification auditors, research bodies, data controllers/processors, operators, service providers, law enforcement agencies, privacy law scholars and social scientists. For the most part, engineers and designers will require certified training in PBD, and manufacturers/developers of PITs will require privacy law experts to further guide and advise their designers and engineers on the steps that are legally required for compliance.

In order to reflect public concerns and public policy considerations, the involvement/participation of citizens and/or of consumers/users, perhaps mostly through representative organizations, in the design of PITs, should also play an important role in the adoption of the final product. As Reidenberg argues, "citizen participation is neces-

[959] Indeed, at a networking session at the ICT Event 2010 in Brussels, which I attended, European Commission staff from the Trust & Security unit expressed their preference or intention to fund a Coordination Action that brings together stakeholders for the purpose of facilitating PBD.

sary so that public values and goals are consistent across the three spheres of law, technology and market behavior and activities" (Reidenberg, 2000). Moreover, PBD could potentially benefit immensely from methods of collaborative design and production with interested citizens and/or consumers, where applicable, appropriate and feasible. The involvement of citizens and/or consumers could also facilitate the legitimacy and trustworthiness of the relevant PITs.

Civil society and privacy commissioners can also help to advocate for the necessary greater public and private investment and cooperation in the R&D of PBD solutions (Cavoukian, 2009) and help to raise public awareness of the emergence of new technologies that pose a threat to privacy and other civil liberties.

If successful, PBD in the end could serve as a bridge between lawmakers, policymakers, practitioners, engineers/designers and academics, and thus potentially evolve into a policy instrument for overcoming the separation of the variety of relevant stakeholders and actors, for minimizing the excessive division of their efforts to protect privacy and for identifying the concurrences, synergies and overlaps of their endeavors.

10.19 LIMITATIONS AND CONSTRAINTS OF PBD

While PBD may be critical for protecting privacy against the intrusive capabilities of the latest technologies, in practice the approach is *not* a panacea for preventing all problems/issues related to privacy intrusion. Certainly, legally mandating that technical solutions be implemented at the earliest stage of development is no magic bullet, not to mention the criticism of PBD (see section 9.11) and the challenges of implementing PBD (see section 9.12). There is simply no magic bullet for completely guaranteeing privacy, nor any single way to completely ensure that governments, companies, data controllers and operators of PITs comply with all privacy laws and principles all the time.

There will certainly still be moments when companies and governments violate privacy and design devices or systems that threaten privacy, whether deliberately or unintentionally, lawfully or unlawfully. After all, PITs are not the really causality of privacy infringement, but rather the means. Human behavior is the cause, and privacy invasion is the effect. It is for that reason why PITs must be designed in a way that regulates human behavior and minimizes the effects of that behavior. But, PBD will certainly not remove the need for doing so.

No matter how PITs are designed/developed, their widespread deployment and use will likely always present concerns over the protection of privacy and liberty. Law does not perfectly regulate behavior and neither does technology. The PBD approach cannot entirely prevent every privacy violation conducted either accidently or intentionally. Just like designing bombs/missiles to be ‘smart’ may be an effective way of better putting into practice the Geneva Conventions on the prohibition of killing civilians indiscriminately during a war, it does not mean that mistakes based on poor intelligence, for example, will not occur, or that militaries will never intentionally use ‘smart bombs’ to kill civilians.

PBD neither can answer nor solve all the critical legal questions. For example, while PBD can aim to develop location-based services and related products for consumer use in a privacy-friendly manner, it cannot determine the lawfulness in the US of warrantless GPS tracking conducted by law enforcement agencies or determine the privacy protections afforded to location information generated by HIMs (or mobiles phones and other PLDs) or the level of privacy afforded to citizens/consumers out in public.

Again, as Sollie and Dowell (2009) argue, an anticipatory outlook is required when addressing new technologies. However, given that the ability of the designers and engineers to imagine or anticipate all future scenarios is limited (Albrechtslund, 2007, p. 72), it is unlikely that all the intended and unintended eventual uses of a particular PIT, and the privacy threats thereof, can be foreseen at all times during the design and development stage or even after a PIA and privacy audit is conducted. For instance, predicting every privacy threat now and in the future will be particularly difficult in a ‘ubiquitous information society’. Any uncertainty or unawareness of all the privacy threats and implications of the technology in question is equally a predicament for PBD, particularly if the technology, device, infrastructure, system or service has never been deployed and used yet. Therefore, since the development of new technologies regularly occurs under conditions of uncertainty, as Sollie and Düwell (2009) point out, then the effectiveness of PBD may equally be uncertain and limited at times.

In addition, as data controllers/processors and service providers increasingly use so many different technologies, devices, tools and systems, determining the specific technical problem or defect, identifying the responsible/liable party and establishing a link between the problem, defect or malfunction and the privacy damage is less and less obvious.[960] For example, a RFID system could be composed of different types of RFID tags and readers, databases, fixed and mobile computing devices and software.[961] As a result of the (potential) lack of a clear understanding of responsibility/liability, the enforcement of PBD requirements will equally face obstacles and constraints.

---

960 see *Trust in the Information Society: Research and Innovation on Security, Privacy and Trustworthiness in the Information Society*, A Report of the Advisory Board RISEPTIS, 2009, p. 13. (RISEPTIS was composed of more than 30 experts and was supported by an EC-financed ‘Coordination Action’ project, THINKTRUST, whose objective was to develop a research agenda for Trustworthy ICT).

961 see Cannataci, Joseph A. *Recent developments in privacy and healthcare: Different paths for RFID in Europe and North America?* (International Journal of RF Technologies, Volume 2, 2010/2011), pp. 173–187.

While PBD can potentially better minimize the impact of the use of PITs by controlling/minimizing the intrusive capability of the technology in the first place, care should be taken not to give the impression that technology developed under certain legal requirements is no longer susceptible to future ethical dilemmas or future technological advancements (Albrechtslund, 2007). PBD is susceptible to the inclination that PITs, or any technology for that matter, are often never really finished developing. As new capabilities are added, further unforeseen privacy implications may result. Though the goal is to design technology to be privacy-friendly in a way that transcends time, however, PBD must be an ongoing process that requires continuous advancement and re-assessment as PITs constantly advance. If PBD is not as dynamic as technological advancement, then just like laws, the PBD approach will also fall behind. For this reason, as pointed out earlier, Hirsch argues that EMS may be a helpful model for PBD, since EMS often entails continuous improvement practices (Hirsch, 2006, pp. 60-63). Even with the methodical implementation of PIAs and PBD, unforeseen threats to privacy could still be encountered. Some PBD solutions themselves might later on result in unexpected privacy implications, as the technical solutions further advance.

In addition, not all PBD solutions will be effective at present or in the future. Some solutions, even those based on the BATs at the time and designed in a way to be ‘future-proof’ as far as possible, could prove deficient or insufficient later on or end up being susceptible to circumvention or even end up failing. As experience has shown, there is no absolute guarantee that any system or device is completely free of vulnerabilities or privacy risks, just as there is essentially no absolutely impenetrable security system or level of software encryption or error-free computer code. Specifically, for instance, as Grimmelmann points out, “software is vulnerable to failure in three related ways: It is *buggy*, it is *hackable*, and it is *not robust*” (Grimmelmann, 2005, p. 1742). Clearly, if a (PBD) software solution is hacked or somehow circumvented, the solution has not acted as an effective constraint (*Ibid*., p. 1731). A number of PETs, for example, developed for ensuring privacy and data security on the Internet, have already failed. During the initial phase, many of the new PBD solutions developed will likely fail or be circumvented.

While PBD solutions for protecting privacy aim to minimize the intrusive capabilities of the technology concerned, PBD cannot address every privacy threat posed by every PIT, since not all privacy threats posed by the latest technologies can be designed or engineered away. As a case in point, PBD is understandably not an all-encompassing solution to dealing with the very complex and dynamic privacy issues surrounding the greater use and advancement of DNA analysis and neurotechnology. Similarly, as Grimmelmann (2005) points out, technology/software cannot implement every rule. Consequently, there are certainly some privacy threats outside the scope of PBD solutions, at least for the time being.

As outlined earlier (see section 10.4), technical and/or PBD solutions alone cannot in practice guarantee privacy, and Lessig's other dimensions/modalities for regulating technology will also play an important role in the success of PBD. For starters, laws that mandate these solutions be implemented, specify the liability of not complying, provide for audit and enforcement mechanisms, provide legal remedies, provide the legal mechanisms to intervene in the chain of production, require the notice and consent of data subjects, and regulate the general deployment and use of PITs are still required. Moreover, PBD alone cannot implement all of the relevant legal requirements. For instance, administrative processes, such as the requirements of organizational accountability and notification requirements, cannot be implemented through PBD (van Blarkom, G.W. et al., 2003, p. 50).

The market dynamics, which in a free market are normally beyond the control of the government, can also limit the success of PBD. The implementation of PBD depends, in part, on the willingness of manufacturers to comply. Since PBD solutions come at an additional cost, in order for PBD to be employed or implemented at an acceptable rate, the developers/manufacturers of PITs must also be convinced and fully aware of the value and financial justification or business benefits in complying and the financial costs, risks and liabilities of meager privacy controls/safeguards. As Borking points out, from a business perspective, it makes no sense to invest in a privacy protecting solution if the actual costs of the solution are greater than the value it actually offers (Borking, 2010, p. 260). The value will increase as consumers increase their demand for privacy-friendly products and services. If consumers persistently continue to demand that their privacy be protected, then so too will the demand for devices, systems and services that are designed in a privacy-friendly manner. However, the success of PBD will require not only companies to view the protection of privacy as profitable or financially justifiable.

The political determination of lawmakers will also decide the extent to which PBD is realized. Reaping the benefits of PBD will equally require constructive political choices in addition to technical choices. Therefore, radically changing the way companies and governments design, develop and procure PITs will require, not just new technological and legal solutions, but the basis to overcome economic and political reservations. Economic reservations can come from the extra costs and burdens of PBD and the political reservations will likely come in the form of hesitations in intervening further in the production chains of free enterprises in a market-driven, laissez-faire economy. Significant investment and resources from both the private and public sector will need to be allocated to carry out the necessary R&D and innovation, in order to realize effective PBD solutions, tools and methods to implement and enforce the relevant privacy principles and laws thereof.

In order to induce politicians to take the necessary steps to pass new comprehensive laws requiring the implementation of PBD in PITs, politicians will need to further recognize the protection of privacy as an additional source of political legitimacy and recognize that it is indeed possible to engineer privacy into PITs. Moreover, like with environmentally-friendly devices, systems and services, the demand for privacy-friendly devices, systems and services will also need to come from governments, and not just consumers. Since governments are significant buyers of PITs, the adoption/implementation of policies in support of the public procurement and pre-commercial procurement of privacy-friendly devices and systems could set a good example and further influence the design and development of PITs. Essentially, as long as the business case and business model is weak and the political will is absent, PBD will not take off, regardless of the legal framework in place.

Finally, the continuation of privacy values and norms and an expectation of privacy are required. Apparently, the "Internet Generation" (or the "Millennial Generation") increasingly has less appreciation and expectation for privacy, and today's teenagers could grow up to future adults who do not care a great deal about their privacy. The Founder and CEO of Facebook, Mark Zuckerberg, also suggested that privacy is already no longer really a social norm and that sharing information instead has become the new norm,[962] without basing his claim on any empirical evidence or statistics.[963] However, Zuckerberg has a vested interest in making this claim, which was anyhow proven, for the most part, erroneous or at least premature, as demonstrated by the uproar of Google Mail (Gmail) users just days after the launch of Google Buzz. Nonetheless, if Zuckerberg's claim ends up proving true, the demand for privacy-friendly devices and services, as a result, could significantly decline. This could also end up diminishing the widespread support and implementation of PBD.

In sum, the general conclusions and policy recommendations of this dissertation, in support of PBD, are indeed limited by the ability of designers and engineers to envi-

---

[962] Gaudin, Sharon. "Facebook CEO Zuckerberg causes stir over privacy" (Computerworld, 11 January 2010), available at: http://www.computerworld.com/s/article/9143859/Facebook_CEO_Zuckerberg_causes_stir_over_privacy?taxonomyId=16

[963] A recent poll has perhaps contradicted Zuckerberg's statement. The Pew Research Center's Internet & American Life Project found that young adults (ages 18-29) in fact are not indifferent about their online reputation. For example, 71% of young adults who are social networking users have changed their account privacy settings in order to limit what they share online. The results were based on data from telephone interviews conducted, between August and September 2009, among a sample of 2,253 young adults in the US. see: Reputation Management and Social Media, Pew Internet and American Life Project, May 2010.
(But, the survey targeted young adults (ages 18-29) and not teenagers. Moreover, there is still relatively little empirical data on society's overall perceptions of privacy and how, why and when it is most valued.)

sion the threats posed by PITs, their ability to design and engineer away the threats to privacy, their ability to keep up with the ever growing threats and intrusive capabilities of PITs, the ability of the legal framework to ensure implementation and compliance, the market dynamics, the consumer demand, the political will of lawmakers, and the persistence of key privacy values and norms.

10.20 FINAL CONCLUSIONS

PBD is the critical combination of technology and law that can potentially propel a legal framework forward to address not just information privacy and the new threats posed by body scanners, RFID/GPS implants and CCTV microphones and loudspeakers, but also the incredible threats to privacy posed by other privacy-intrusive technologies. Adequate technical and design solutions, based on the well-established principles of privacy, can potentially convert the unrestrained, radical privacy-intrusive capabilities of these technologies into prudent, privacy-friendly commercial and security gains.

For far too long, manufacturers/developers of PITs have been generally ignored by data protection/privacy legislation and, as a consequence, the laws have often fallen behind new technological developments and have failed to address the privacy-intrusiveness of the technologies concerned at the design stage. Instead, new laws should mandate that the designers and developers of these technologies implement PBD solutions, where appropriate, and punish those who fail to do so. Accordingly, more burdens will be placed on the designers and developers of these technologies, rather than overly relying on the goodwill and compliance of the data controllers, service providers and operators/users of these technologies. As a result, the legal framework may be better equipped to stay apace with the rapidly changing and advancing technological threats to privacy.

Moreover, for far too long, the protection of privacy in the US and UK has been at the mercy of the legal interpretations of courts to fill-in the gaps and/or to address the legal issues or deficiencies of existing data protection/privacy legislation. Instead of excessively relying on the sometimes altering and inconsistent legal interpretations of courts, comprehensive PBD legislation can bring about the required consistency and permanence.

In conclusion, PBD is arguably the best option there is, at present, to balance the (potential) trade-offs between privacy and liberty, on the one hand, and public security, convenience and commerce, on the other. While it is not necessarily possible to prevent every conceivable violation of the right to privacy or fully address every threat to privacy, it is reasonably evident that practically any device or system is more likely not to jeopardize privacy and liberty if it is legally required to be designed and manufactured with the relevant privacy principles built-in than if it is not required so. Although technology/technical solutions cannot completely guarantee privacy and liberty, it can at least provide the circumstances and environment in which privacy and liberty stand a much better chance in the modern world. At the same time, technology will certainly still present challenges to privacy and civil liberties, albeit these challenges can be better managed and addressed through PBD.

Nonetheless, the dire reality is that the diminishment of privacy or the serious threats to privacy posed by the inertia of technological development run rampant is probably an issue just too big for PBD or any single legal or technical solution alone. But, taking no action is not an option either, as society is faced with increasing threats to privacy posed by the evermore advancement and deployment of PITs. The realistic objective of PBD is to separate the problem into achievable legal, policy and technical options for addressing the threats posed by the latest technologies now and in the future. However, with the evermore advancement of privacy-threatening technologies, in any case, probably the best we can hope for and strive to achieve for now is at least to defend privacy and liberty for the foreseeable part of the 21st Century.

ANNEX I: A3 Report

PROBLEM

Technology, meant to improve the security and wellbeing of citizens, is posing a serious threat to privacy and liberty. If privacy and individual liberty are as dangerously at stake as easy to infringe upon, then the rapid and continuous technological advancement of PITs has and will increasingly continue to seriously jeopardize civil liberties.

CURRENT CONDITIONS

Privacy laws are not adequate to safeguard privacy and liberty against the privacy-intrusive capabilities of the latest technologies.
- Why? The law does not ensure the enforcement of the fundamental principles of privacy for the latest PITs.
- Why? The legal framework is outdated.
- Why? The law is behind the technology, as technology is rapidly developing faster than the law.
- Why? Law making is generally a slow process and privacy laws are not concerned with having an influence on the development of technology.
- Why? Law making is primarily reactive or ex-post.

COUNTERMEASURES

- Amendments and enhancements to the current legal framework;
- Rules and regulations on the development of PITs;
- Technological / design solutions for protecting privacy.

ACTION PLAN

- Assess the legal framework against the criteria of adequacy;
- Identify the crucial deficiencies and dilemmas in the respective legal frameworks where applicable;
- Determine the necessary new laws, legal definitions, safeguards and interpretations, and technological and design solutions to minimize the impact on privacy brought about by the latest PITs;
- Develop criteria for evaluating the truthfulness and adequacy of the privacy
- protection assertions of PITs concerned;
- Accordingly, adopt and pass new and comprehensive legislation on privacy.

DESIRED OUTCOME

A legal and policy framework that effectively balances privacy and liberty on the one hand and security on the other, ensures privacy protection law is up to date for many years to come, regardless of the technology concerned, and combines binding legal solutions with technological solutions, mandating that PITs are designed and developed manufactured with the principles of privacy taken into consideration proactively or ex-ante.

FOLLOW-UP/IMPLEMENTATION

- Invest in the R&D of privacy by design solutions (Government and private sector);
- Establish a certification scheme to audit the adequacy of the PBD solutions for PITs, inaccordance with the new law (Government);
- Identify the foreseeable privacy threats and vulnerabilities of the PITs concerned (as far as possible) and assess the potential risks involved (Developers of the PITs concerned).

ANNEX II: Summary Table

Privacy-Invading Technologies	**Body Scanners (US)**	**RFID implants (US)**
Intrusive Capabilities	Enables the conduct of a 'virtual' strip search or the operator to see just beneath a person's clothes.	Enables the automatic identification and/or tracking of individuals.
Most Relevant Laws (Statutory laws and jurisprudence)	Fourth Amendment of the US Constitution; Federal Rules of Legal Evidence; E-Government Act of 2002; Katz v. United States (1967); United v. Epperson (4th Circuit, 1972); United States v. Skipwih (5th Circuit 1973); United States v. Ramsey (1977); Harlow v. Fitzgerald (1982); United States v. Knotts (1983); United Stats v. Vega-Barvo (11th Circuit, 1984); Justice v. City of Peachtree City (11th Circuit, 2001); Kyllo v. United States (2001); Brent v. Ashley (11th Circuit, 2001); Amaechi v. West (4th Circuit, 2001).	FTC Act; Privacy Act of 1974; California SB 362; North Dakota SB 2415; Wisconsin Statute 146.25; The Restatement (Second) of Torts; Katz v. United States (1967); United States v. Karo (1984); Oliver v. United States (1984); Kyllo v. United States (2001).
Most Relevant Self-regulations/ Codes/ Guidelines	TSA self-regulations.	AMA medical code of ethics; VeriChip's privacy policy.
Most Significant Legal Deficiencies	Strip search legally involves the removal of clothes; the relevant legal framework is: ambiguous, fails to uphold the privacy principles, unforeseeable, and is over-dependent on altering, non-legally binding self-regulations.	No federal law regulating RFID; forced vaccinations are potentially lawful; no legal recognition of the privacy of a person's movements out in public; the Privacy Act of 1974 is not applicable to HIM service providers.
Key recommendations and proposed legal/ technological solutions	Software algorithms; built-in restrictions on the capabilities of body scanners; amendment of the definition of a strip search; dedicated supervision/oversight; harden the self-regulations of the TSA.	Implementation of privacy principles; new definition of location information; legal recognition of 'public privacy'; criminal penalties for eavesdropping on RFID implants; application of the Fourth Amendment to location information; HIM purpose declarations; the incorporation of privacy principles at the reader-to-tag protocol level; encryption; a web interface.

Privacy-Invading Technologies	GPS implants (US)	Public space CCTV microphones (UK)
Intrusive Capabilities	Enables the accurate, real time tracking of a person's movements.	Enables the audio recording of conversations out in public.
Most Relevant Laws (Statutory laws and jurisprudence)	Telecom Act of 1996; Federal Rules of Criminal Procedure; CALEA; ECPA; Title 47 U.S.C. Chapter 5, Subchapter II, Part I, § 222; Title 18 U.S.C. Part II, Chapter 205, § 3117(b); Title 47 C.F.R. Ch. I, § 20.18; Wireless Communications and Public Safety Act of 1999; Report and Order and Further Notice of Proposed Rulemaking, FCC 07-22; Title 47 C.F.R. § 64.2003(k); Katz v. United States (1967); United States v. Karo (1984); Oliver v. United States (1984); Kyllo v. United States (2001); United States v. Garcia (7th Circuit, 2007); State of Wisconsin v. Michael A. Sveum (District of Wisconsin Court of Appeals, 2009); United States v. Jones (2012).	Directive 95/46/EC; Data Protection Act 1998; Human Rights Act 1998; ECHR; Durant v. Financial Services Authority (2003); Private Security Industry Act 2001.
Most Relevant Self-regulations/ Codes/ Guidelines	CTIA Best Practices and Guidelines for LBS; GIS Code of Ethics.	CCTV code of practice 2008.
Most Significant Legal Deficiencies	GPS tracking is currently not considered a search and is permitted without a warrant; no clarity on the level of suspicion required to conduct tracking and/or access location information; the Telecom Act offers no protection to location information generated by devices other than cell phones.	The narrowed legal definition of personal data; the DPA does not cover general sound recorded in public; CCTV code of practice is ambiguous and not legally binding; legally little or no privacy out in public.
Key recommendations and proposed legal/ technological solutions	Implementation of the privacy principles; new comprehensive definition of location information; nationwide breach notification; legal recognition of 'public privacy'; reformulation of relevant tort law; criminal penalties for unauthorized monitoring or interception of GPS implants; amendments to the ECPA; application of Fourth Amendment protections to location information and GPS tracking; HIM purpose declarations.	Limit the activation of the CCTV microphones to specific sounds using incorporated artificial intelligence.

Privacy-Invading Technologies	Public space CCTV loudspeakers (UK)
Intrusive Capabilities	Gives CCTV control room operators the ability to violate an individual's right to be left alone.
Most Relevant Laws (Statutory laws and jurisprudence)	Crime and Disorder Act 1998; Regulation of Investigatory Powers Act 2000; Anti-Social Behaviour Act 2003.
Most Relevant Self-regulations/ Codes/ Guidelines	CCTV code of practice 2008.
Most Significant Legal Deficiencies	CCTV code of practice fails to define the circumstances of the legitimate use of CCTV loudspeakers; RIPA is ambiguously worded and permits broad abuse.
Key recommendations and proposed legal/ technological solutions	Limitations on the use of CCTV loudspeakers to pre-recorded messages; disciplinary action for abuse; an oversight committee.

References

BOOKS

Albrecht, Katherine and McIntyre, Liz. *Spychips: How Major Corporations and Government Plan to Track Your Every Move with RFID* (Thomas Nelson, 2005).

Agre, Philip E. and Marc Rotenberg (eds.), *Technology and Privacy: The New Landscape* (MIT Press, 1997).

Bennett, Colin. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Cornell University Press, 1992).

Berger, Warren. *Glimmer: How Design Can Transform Your Life and Maybe Even the World* (Penguin Press, 2009).

Berlin, Isaiah. *Two Concepts of Liberty* (Oxford University, 1958).

Billig, Michael. *Banal Nationalism* (Sage Publications, 1995).

Brin, David. *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* (Basic Books, 1999).

Brzezinski, Zbigniew. *Between Two Ages: America's Role in the Technetronic Era* (Penguin Books, 1976).

Cavoukian, Ann. *Privacy by Design* (2009).

Etzioni, Amitai. *The limits of privacy* (Basic Books, 1999).

Feldman, David. *Civil Liberties and Human Rights in England and Wales* (Oxford University Press, 2002).

Foucault, Michel. *Power/Knowledge: Selected Interviews and Other Writings, 1972-1977* (Pantheon, 1980)

Garfinkel, Simson. *Database Nation: The Death of Privacy in the 21st Century* (O'Reilly Media, 2001).

Greenfield, Adam. *Everyware: The Dawning Age of Ubiquitous Computing*, (New Riders Publishing, 2006).

Friedman, B., Kahn, P.H. and Borning, A. *Value Sensitive Design: Theory and Methods* (University of Washington, 2002).

Furedi, Frank. *Culture of Fear Revisited: Risk-taking and the Morality of Low Expectation* (Continuum, 2006).

Harris, D., O'Boyle, K. and Warbrick C. *Law of the European Convention on Human Rights* (Sweet & Maxwell, 1995).

Holtzman, David H. *Privacy Lost: How Technology Is Endangering Your Privacy* (Jossey-Bass, 2006).

Hood, Leroy and Lee Rowen. *Genes, Genomes, and Society, Genetic Secrets: Protecting Privacy and Confidentiality in the Genetic Era* (ed.) Mark A. Rothstein (Yale University Press, 1997).

Hunt, V. Daniel., Albert Puglia, and Mike Puglia. *RFID-A Guideline to Radio Frequency Identification* (Wiley, 2007).

Kurzweil, Ray. *The age of intelligent machines* (MIT Press, 1990).

Lessig, Lawrence. *Code and Other Laws of Cyberspace* (Basic Books, 1999).

Long, Edward V. *The Intruders: The Invasion of Privacy by Government and Industry* (Praeger, 1967).

Lyon, David. *Surveillance society: monitoring everyday life* (Open University Press, 2001).

Merriam-Webster's Dictionary of Law (1996).

Monmonier, Mark S. *Spying with maps: Surveillance Technologies and the Future of Privacy* (University Of Chicago Press, 2004).

Norris, C. and Armstrong, G. *The Maximum Surveillance Society: The Rise of CCTV* (Oxford, 1999).

O'Hara, Kieron and Nigel Shadbolt. *The Spy in the Coffee Machine: The End of Privacy As We Know It* (Oneworld publications, 2008).

O'Harrow, Robert. *No place to hide* (Free Press, 2005).

Orwell, George. *Nineteen Eighty-Four* (Secker and Warburg, 1949).

Paley, William. *The Principles of Moral and Political Philosophy* (R. Faulder, 1785).

Regan, Priscilla M. *Legislating Privacy: Technology, Social Values, and Public Policy* (University of North Carolina Press, 1995).

Schermer, B.W. *Software agents, surveillance, and the right to privacy: a legislative framework for agent-enabled surveillance* (PhD diss., Leiden University Press, 2007).

Smith, Adam. *An Inquiry into the Nature and Causes of the Wealth of Nations* (Methuen & Co., Ltd., 1904, 5th edition, first published 1776).

Sollie, Paul and Marcus Duwell (eds.)., *Evaluating New Technologies: Methodological Problems For The Ethical Assessment Of Technology Developments* (Springer, 2009).

Solove, Daniel. *The Digital Person: Technology and Privacy in the Information Age* (New York University Press, 2004).

Solove, David. *Understanding Privacy* (Harvard University Press, 2008).

Stephen, James Fitzjames. *Liberty, Equality, Fraternity* (London, 1873).

Sterling, Bruce. *Shaping Things* (MIT Press, 2005).

Tamanaha, Brian Z. *On the Rule of Law: History, Politics, Theory* (Cambridge University, 2004).

Wacks, Raymond. *The protection of privacy.* (Sweet & Maxwell, 1980).

Westin, Alan. *Privacy and Freedom* (Atheneum, 1967).

Whitaker, Reg. *The End of Privacy: How Total Surveillance Is Becoming a Reality* (New Press, 2000).

PUBLISHED PAPERS

Aarts, Emile., and Boris de Ruyter. *New research perspectives on Ambient Intelligence* (Journal of Ambient Intelligence and Smart Environments I, 2009), pp. 5-14.

Albrechtslund, Anders. *Ethics and technology design* (9 Ethics and Information Technology, 2007), pp. 63-72.

Ayoade, John. *Roadmap to solving security and privacy concerns in RFID systems* (Computer Law & Security Report, Volume 23, Issue No. 6, 2007), pp. 555-561.

Bannister, J., Fyfe, N. and Kearns, A. "Closed Circuit Television and the City", in C. Norris, J. Moran and G. Armstrong (eds.), *Surveillance, Closed Circuit Television and Social Control* (Ashgate, 1998).

Barbat, Boldur., Andrei Moiceanu, Hermina Anghelescu. "Enabling Humans to Control the Ethical Behaviour of Persuasive Agents" in Eugene Loos, Leslie Haddon and Enid Mante-Meijer (eds.), *The social dynamics of information and communication technology* (Ashgate, 2008).

Beslay, Laurent., and H. Hakala. "Digital Territory: bubbles" in Paul T. Kidd (ed.) *European Visions for the Knowledge Age: A Quest for New Horizons in the Information Society* (Cheshire Henbury, 2007).

Bignami, Francesca. *The Non-Americanization of European Regulatory Styles: Data Privacy Regulation in France, Germany, Italy, and Britain* (Center for European Studies Working Paper Series #174, 2010), available at: http://www.ces.fas.harvard.edu/publications/docs/pdfs/CES_174.pdf

Birnhack, Michael D. *The EU Data Protection Directive: An Engine of a Global Regime* (Tel Aviv University Law Faculty Papers, Paper 95, 2008).

Borking, John. "Assessing investments mitigating privacy risks" in Laurens Mommers, Hans Franken, Jaap van den Herik, Franke van der Klaauw and Gerrit-Jan Zwenne (eds.) *Het binnenste buiten; Liber amicorum ter gelegenheid van het emeritaat van Prof.dr.Aernout H.J.Schmidt, Hoogleraar Recht en Informatica te Leiden* (eLaw@ Leiden, 2010), pp. 255-273.

Brownsword Roger. *Code, control and choice: why East is East and West is West* (Legal Studies, Volume 25, Issue No 1, 2005), pp. 1-21.

Cannataci, Joseph A. *Squaring the Circle of Smart Surveillance and Privacy* (Proceedings of the 2010 Fourth International Conference on Digital Society, IEEE Computer Society 2010).

Cannataci, Joseph A. *Recent developments in privacy and healthcare: Different paths for RFID in Europe and North America?* (International Journal of RF Technologies, Volume 2, 2010/2011), pp. 173–187.

Cannataci, Joseph A. *Lex Personalitatis: Personality, Law and Technology in the 21st Century* (Acta Universitatis Lucian Blaga 219, 2008).

Cockfield, Arthur I. *Who Watches the Watchers? A Law and Technology Perspective on Government and Private Sector Surveillance* (29 Queen's Law Journal, 2003), pp. 364-407.

Cooper, Joshua and Anne James. C*hallenges for Database Management in the Internet of Things* (IETE Technical Review, Vol. 26, Issue No. 5, August 2009), available at: http://tr.ietejournals.org/text.asp?2009/26/5/320/55275

Dick, Danielle M., et al. *Association of CHRM2 with IQ: Converging Evidence for a Gene Influencing Intelligence* (Behavior Genetics, Vol. 37, No. 2, March 2007), pp. 265-272.

Dobson, Jerome E. and Fisher, Peter F. *Geoslavery* (IEEE Technology and Society Magazine, 2003).

Dommering, Egbert. "Regulating technology: Code is not law", in E.J. Dommering & L.F. Asscher (eds.) *Coding Regulation: Essays on the Normative Role of Information Technology* (T.M.C. Asser Press, 2006), pp. 1-17.

Donohue, Laura K. *Anglo-American Privacy and Surveillance* (Journal of Criminal Law & Criminology, Vol. 96, No. 3, 2006), pp. 1059-1208.

Dubnikova, Faina., et al. *Decomposition of Triacetone Triperoxide Is an Entropic Explosion* (Journal of the American Chemical Society, January, 2005).

Duncan, George. *Engineering: Privacy by Design* (Science, Vol. 317. No. 5842, August 2007), pp. 1178-1179.

Edmundson, Kristen E. *Global Positioning System Implants: Must Consumer Privacy Be Lost in order for People to be Found* (38 Indiana Law Review 207, 2005), pp. 207-238.

Emmett, Caitlin. *United States v. Pineda-Moreno, Tracking Down Individuals' Reasonable Expectation of Privacy in the Information Age* (41 Golden Gate University Law Review, 2011).

Epstein, Jules. *"Genetic Surveillance" - The Bogeyman Response to Familial DNA Investigations* (Journal of Law, Technology and Policy, Vol. 2009, No. 1), pp. 141-173.

Flanagan, M., D. Howe and H. Nissenbaum. "Embodying Values in Design: Theory and Practice" in J. van den Hoven and J. Weckert (eds.), *Information Technology and Moral Philosophy* (Cambridge University Press, 2008).

Feldhofer M., S. Dominikus and J. Wolkerstorfer *Strong authentication for RFID systems using the AES algorithm* (Proceedings of CHES in LNCS, Volume 356, 2004).

Feldman, David. *Secrecy, Dignity or Autonomy? Views of Privacy as a Civil Liberty* (47 Current Legal Problems 41, 1994).

Floerkemeier, Christian., et al. *Scanning with a Purpose – Supporting the Fair Information Principles in RFID Protocols* (Distributed Systems Group, Swiss Federal Institute of Technology, 2005).

Frumkin, Dan., et al. *Authentication of Forensic DNA samples* (Forensic Science International: Genetics, 2009).

Ganz, John S. *It's Already Public: Why Federal Officers Should Not Need Warrants to Use GPS Tracking Devices* (95 The Journal of Criminal Law and Criminology, 2005).

Garfinkel, Simson L., Ari Juels and Ravi Pappu. *RFID privacy: an overview of problems and proposed solutions* (IEEE Security and Privacy, Volume 3, Issue 3, May 2005), pp. 34-43.

Gavison, Ruth. *Privacy and the Limits of Law* (The Yale Law Journal, Volume 89, No. 3, Jan. 1980), pp. 421-471.

Goold, Benjamin J. *Open to All - Regulating Open Street CCTV and the Case for Symmetrical Surveillance* (25 Criminal Justice Ethics, 2006), pp. 3-17.

Grimmelmann, James. *Regulation by Software* (Yale Law Journal, Volume 114, 2005), pp. 1719-58.

Guarda, Paolo., and Nicola Zannone. *Towards the development of privacy-aware systems* (Information and Software Technology, Volume 51, Issue 2, February 2009), pp. 337-350.

Gutterman, Melvin. *A Formulation of the Value and Means Models of the Fourth Amendment in the Age of Technologically Enhanced Surveillance* (39 Syracuse Law Review 647, 1988).

Gutwirth, Serge., Paul De Hert,. and Laurent De Sutter. "The trouble with technology regulation from a legal perspective. Why Lessig's 'optimal mix' will not work" in Brownsword, R. and Yeung, K. (eds.) *Regulating Technologies* (Hart Publishers, 2008), pp. 193-218.

Haggerty, Kevin D. and Richard V. Ericson. *The Surveillant Assemblage* (British Journal of Sociology, Vol. 51, Issue No. 4, December 2000), pp. 605–622.

Halamka, John., et al. *The Security Implications of VeriChip Cloning* (Journal of the American Medical Informatics Association, Volume 13, Issue 6, 2006), pp. 601-607.

Herbert, William A. *No Direction Home: Will the Law Keep Pace With Human Tracking Technology to Protect Individual Privacy and Stop Geoslavery* (I/S: A Journal of Law and Policy for the Information Society, 2006), pp. 409-473.

Hes, Ronald. and John Borking (eds.), P*rivacy-Enhancing Technologies: The path to anonymity* (Registratiekamer, The Hague, August 2000).

Hilbert, Martin. *The end justifies the definition: the manifold outlooks on the digital divide and their practical usefulness for policy-making* (Telecommunications Policy, Volume 35, Issue 8, 2011), pp. 715-736.

Hildebrandt, Mireille. and Bert-Jaap Koops. *The Challenges of Ambient Law and Legal Protection in the Profiling Era* (Modern Law Review, Vol. 73, Issue 3, May 2010), pp. 428-460.

Hildebrandt, Mireille. "Technology and the end of law" in Erik Claes, Wouter Devroe, Bert Keirsbilck (eds.), *Facing the limits of the law* (Springer, 2009), pp. 443-464.

Hinson, Zoila. *GPS monitoring and constitutional rights* (43 Harvard Civil Rights-Civil Liberties Law Review, 2008), pp. 285-288.

Hirsch, Dennis D. *Protecting the Inner Environment: What Privacy Regulation Can Learn from Environmental Law* (41 Georgia Law Review 1, 2006), pp. 1-64.

Hirsch, Dennis. *Law and Policy of Online Privacy: Regulation, Self-Regulation or Co-Regulation* (Seattle University Law Review, Vol. 34, Issue 2, 2011), pp. 439-480.

Hubbard, Robert W., Magotiaux, Susan and Sullivan, Matthew. *The State Use of Closed Circuit TV: Is There a Reasonable Expectation of Privacy in Public* (Criminal Law Quarterly, Volume 49, Issue No. 2, 2004), pp. 222-250.

Hutchins, Renee. *Tied Up in Knotts? GPS Technology and the Fourth Amendment* (UCLA Law Review, Volume 55, No. 1, 2007), pp. 409-465.

Karat, John., Clare-Marie Karat, Carolyn Brodie and Jinjuan Feng. *Privacy in information technology: Designing to enable privacy policy management in organizations* (International Journal of Human-Computer Studies, Volume 63, Issues 1-2, July 2005), pp. 153-174.

Karim, Waseem. *The Privacy Implications of Personal Locators: Why You Should Think Twice Before Voluntarily Availing Yourself to GPS Monitoring* (14 Washington University Journal of Law and Policy, 2004), pp. 485-515.

Kearns, Thomas B. *Technology and the Right to Privacy: The Convergence of Surveillance and Information Privacy Concerns* (7 William & Mary Bill of Rights Journal, 1998).

Kenny, Steve. and John Borking. *The value of privacy engineering* (Journal of Information, Law and Technology 2, 2002).

Kim, Yongjun, et al., "Sound Detection as an Aid to Increase Detectability of CCTV in Surveillance System", in Nural Aykin (ed.) *Usability and Internationalization* (Springer-Verlag Berlin Heidelberg, LNCS, Vol. 4560, 2007), pp. 382–389.

King, Jennifer and Chris Jay Hoofnagle. *A Supermajority of Californians Supports Limits on Law Enforcement Access to Cell Phone Location Information* (April, 2008).

Kirby, Hon Justice Michael. *Privacy protection, a new beginning: OECD principles 20 years on* (Privacy Law and Policy Report, Volume 6, No. 3), pp. 25-29, available at: http://www.austlii.edu.au/au/journals/PLPR/1999/41.html

Langheinrich, M. "Privacy by Design – Principles of Privacy-Aware Ubiquitous Systems", in G. D. Abowd, B. Brumitt and S. A. Shafer (eds.), *Proceedings of the Third International Conference on Ubiquitous Computing*, Ubicomp 2001, (Springer-Verlag, 2001), pp. 273-91.

Leenes, R., and B.J. Koops. *'Code': Privacy's Death or Saviour?* (International Review of Law, Computers & Technology, Volume 19, No. 3, 2005), pp. 239-340.

Little, Linda., Pam Briggs and Lynne Coventry. *Public space systems: Designing for privacy*? (International Journal of Human-Computer Studies, Volume 63, Issues 1-2, July 2005), pp. 254-268.

Masters, A. and K. Michael. *Lend me your arms: the use and implications of human-centric RFID* (Faculty of Informatics, University of Wollongong, 2006).

Mazerolle, Lorraine Green et al. *Random Gunfire Problems and Gunshot Detection Systems* (National Institute of Justice, December 1999).

McClurg, Andrew J. *Bringing privacy law out of the closet: a tort theory of liability for intrusions in the public space* (73 North Carolina Law Review, 1995), pp. 989-1088.

McGuffin, Peter, Brien Riley and Robert Plomin. *Genomics and Behavior: Toward Behaviorial Genomics* (Science, Vol. 291, No. 5507, February 2001), available at: http://www.sciencemag.org/cgi/content/full/291/5507/1232

Meyer, H.J., et al. *Implantation of radio frequency identification device (RFID) microchip in disaster victim identification (DVI).* (Forensic Science International, Volume 157, Issue 2, 2006), pp. 168-71.

Michael, K., A. McNamee, M.G. Michael and H. Tootell. *Location-Based Intelligence – Modeling Behavior in Humans using GPS* (Faculty of Informatics, University of Wollongong, 2006).

Minert, Steven R. *Square Pegs, Round Hole: The Fourth Amendment and Preflight Searches of Airline Passengers in a Post-9/11 World* (Brigham Young University Law Review, 2006).

Mock, Tobias W. *The TSA's New X-Ray Vision: The Fourth Amendment Implications of "Body Scan" Searches at Domestic Airport Security Checkpoints* (49 Santa Clara Law Review, 2009), pp. 213-252.

Moreham, N.A. *Privacy in Public Places* (Cambridge Law Journal, 65, 2006), pp 606-635.

Naselaris, Thomas et al. *Bayesian Reconstruction of Natural Images from Human Brain Activity* (Neuron, Volume 63, Issue 6, pp. 902-915, 24 September 2009).

Neocleous, Mark. *Security, Liberty and the Myth of Balance: Towards a Critique of Security Politics* (Contemporary Political Theory, Vol. 6, No. 2, 2007), pp. 131–149.

Nissenbaum, Helen. *Privacy as Contextual Integrity* (Washington Law Review, Vol. 79, No. 1, 2004), pp. 101-140.

Paton-Simpson, Elizabeth. *Privacy and the Reasonable Paranoid: The Protection of Privacy in Public Places* (50 University of Toronto Law Journal 305, 2000).

Porter, Michael & Claas van der Linde. *Green and Competitive* (Harvard Business Review, Sept.-Oct. 1995), pp. 120-134.

Posner., Richard. *The economics of privacy* (American Economic Review, Vol. 71, Issue 2, 1981), pp. 405-409.

Ramesh, Elaine M. *Time Enough? Consequences of Human Microchip Implantation* (Franklin Pierce Law Center, 1997), available at: http://www.fplc.edu/risk/vol8/fall/ramesh.htm.

Rapper, Brian. *Assessing the Technologies of Political Control* (36 Journal of Peace Research, 1999).

Reidenberg, Joel R. *Privacy Protection and the Interdependence of Law, Technology and Self-Regulation* (2000), available at: http://reidenberg.home.sprynet.com/Interdependence.htm

Reidenberg Joel. *Lex Informatica: The Formulation of Information Policy Rules Through Technology* (Texas Law Review, Volume 76, No. 3, 1998), pp 553-93.

Rempell, Scott. *Privacy, Personal Data and Subject Access Rights in the European Data Directive and Implementing UK Statute: Durant v. Financial Services Authority as a Paradigm of Data Protection Nuances and Emerging Dilemmas* (18 Florida Journal of International Law, 2006), pp. 807-842.

Reneger, Aaron. *Satellite Tracking and the Right to Privacy* (53 Hastings Law Journal, 2002).

Schwartz, Paul M. *Beyond Lessig's code for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices* (Wisconsin Law Review, Volume 2000, Issue No. 4, 2000), pp. 743-787.

Schwartz, Paul M., *Privacy and Democracy in Cyberspace* (Vanderbilt Law Review, Volume 52, 1999).

Schermer, Bart. "Privacy and Singularity: little ground for optimism? in Laurens Mommers, Hans Franken, Jaap van den Herik, Franke van der Klaauw and Gerrit-Jan Zwenne (eds.) *Het binnenste buiten; Liber amicorum ter gelegenheid van het emeritaat van Prof.dr.Aernout H.J.Schmidt, Hoogleraar Recht en Informatica te Leiden* (eLaw@ Leiden, 2010), pp. 305-319.

Schmidt, A.H.J. and Franken, H. "Law as code, code as law - general remarks on legal requirements engineering", in H.J. Snijders & S. Weatherill (eds.), *E-commerce Law. National and Transnational Topics and Perspectives.* (Kluwer Law International, 2003), pp. 117-139.

Smith, G. *Behind the Screens: Examining Constructions of Deviance and Informal Practices among CCTV Control Room Operators in the UK* (2 Surveillance & Society, 2/3, 2004), pp. 376-395.

Solove, David. *A Taxonomy of Privacy* (University of Pennsylvania Law Review, Vol. 154, No. 3, 2006), pp. 477-560.

Spiekermann, Sarah. "The RFID PIA – developed by industry, agreed by regulators" in David Wright and Paul de Hert (eds.), *Privacy Impact Assessment: Engaging Stakeholders in Protecting Privacy* (Springer, 2012).

Spivey, Crystal. *Breathing New Life Into HIPAA's UHID – Is The FDA's Green Light To The VeriChip™ The Prince Charming Sleeping Beauty Has Been Waiting For?* (9 DePaul Journal of Health Care Law, 2005-06), pp. 1317-1342.

Surette, Ray. *The thinking eye: Pros and cons of second generation CCTV surveillance systems* (Policing: An International Journal of Police Strategies & Management, 2005, Vol. 28, Iss: 1), pp.152 – 173.

Taylor, Nick. *You've Been Framed: The Regulation of CCTV Surveillance* (7 Journal of Civil Liberties 2, 2002), pp. 83-107.

Taylor, Nick. *State Surveillance and the Right to Privacy* (Surveillance & Society 1, 2002a), pp. 66-85.

Thevissen, Patrick., et al. Implantation of an RFID-tag into human molars to reduce hard forensic identification labor (Forensic Science International, Volume 159, 2006), pp. 33-39.

Tien, Lee. *Architectural Regulation and the Evolution of Social Norms* (International Journal of Communications Law & Policy, Issue 9, Autumn 2004).

Tzanou, Maria. *The EU as an Emerging Surveillance Society: The Function Creep Case Study and Challenges to Privacy and Data Protection* (4 Vienna Online Journal on International Constitutional Law, 2010).

van den Hoven, J. "ICT and Value Sensitive Design", in P. Goujon, Lavelle, S., Duquenoy, P., Kimppa, K., Laurent, V., (eds.), The Information Society: Innovations, Legitimacy, Ethics and Democracy (IFIP International Federation for Information Processing, Volume 233, Springer, 2007).

Vina, Stephen R. *Virtual Strip Searches at Airport: Are Border Searches Seeing Through the Fourth Amendment?* (8 Texas Wesleyan Law Review, 2001-2002), pp. 417-439.

Walden, Ian. *Anonymising Personal Data* (International Journal of Law and Information Technology, Vol. 10, Issue 2, 2002), pp. 224-237.

Waldron, Jeremy. *Security and Liberty: The Image of Balance* (Journal of Political Philosophy, Vol. 11, No. 2, 2003), pp. 191-210.

Warner, Richard. *Surveillance and the Self: Privacy, Identity, and Technology* (DePaul Law Review, Vol. 54, No. 3, Spring 2005), pp. 847-71.

Warren, Samuel D. and Louis D. Brandeis. *The Right to Privacy* (Harvard Law Review, Vol. IV, No. 5, 1890), pp. 193-220.

Welsh, Brandon C. and David P. Farrington. *Surveillance for Crime Prevention in Public Space: Results and Policy Choices in Britain and America* (Criminology and Public Policy, Volume 3, No. 4, 2003-2004), pp. 497-526.

Weiser, Mark. *The Computer for the Twentieth-First Century* (Scientific American, Vol. 265, No. 3, September 1991), pp. 94-104.

Werner, Matthew. *Google and Ye Shall Be Found: Privacy, Search Queries, and the Recognition of a Qualified Privilege* (34 Rutgers Computer & Technology Law Journal 313, 2008).

Willingham, Kristina M. *Scanning Legislative Efforts: Current RFID Legislation Suffers from Misguided Fears,* North Carolina Banking Institute Innovative Products, Volume 11, 2007), pp. 313-341.

Yeung, Karen and Mary Dixon-Woods. *Design-based regulation and patient safety: A regulatory studies perspective* (Social Science & Medicine, Volume 71, Issue no. 3, 2010), pp. 502-509.

Yueh-Hsuan Weng, Chien-Hsun Chen and Cheun-Tsai Sun. "Safety Intelligence and Legal Machine Language-Do we need the Three Laws of Robotics?", in Yoshihiko Takahashi (ed.) *Service Robot Applications* (InTech Education & Publishing, August 2008), available at: http://works.bepress.com/weng_yueh_hsuan/3

OTHER PAPERS

Clark, Wesley. *Cell Phone Tracking and Physical Surveillance* (FBI Law Enforcement Bulletin, 2006), available at: http://www.fbi.gov/publications/leb/2006/may06leb.pdf

Juels, Ari and John Brainard. *Soft blocking: Flexible blocker tags on the cheap*, Workshop on Privacy in the Electronic Society (WPES 04), ACM Press, 2004, pp. 1-7.

Kindberg, Tim., et al. *People, Places, Things: Web Presence for the Real World* (Internet and Mobile Systems Laboratory, HP Laboratories Palo Alto, HPL-2000-16, February, 2000), available at: http://www.hpl.hp.com/techreports/2001/HPL-2001-279.pdf

Koops, Bert-Jaap. *Criteria for Normative Technology: An Essay on the Acceptability of 'Code as Law' in Light of Democratic and Constitutional Values* (Tilburg University Legal Studies, Working Paper No. 007/2007, 2007).

Miller, Neal. *Stalking Laws and Implementation Practices: A National Review for Policymakers and Practitioners* (2001), available at: http://www.ncjrs.gov/pdffiles1/nij/grants/197066.pdf

Morris, S., A. Morris and K. Barnard. "Digital Trail Libraries", Joint ACM/IEEE Conference on Digital Libraries, Arizona, 2004, pp. 63-71.

Murphy, Douglas., and James Cycon. "Applications for mini VTOL UAV for law enforcement", available at: http://www.spawar.navy.mil/robots/pubs/spie3577.pdf

Patrick, A.S., and Kenny, S. *From Privacy Legislation to Interface Design: Implementing Information Privacy in Human-Computer Interfaces*. Paper presented at the Privacy Enhancing Technologies Workshop (PET2003), Dresden, Germany, 26-28 March, 2003.

Rastogi, V., et al. "Expressing Privacy Policies Using Authorization Views", Workshop on Ubicomp Privacy, Ubicomp 2007, September 2007, available at: http://rfid.cs.washington.edu/images/rastogi-ubipriv-07.pdf

Rieback, M.R., et al. *RFID Viruses and Worms* (Department of Computer Science, Vrije Universiteit Amsterdam, 2006), available at: http://www.rfidvirus.org

Sandler, Karen., Lysandra Ohrstrom, Laura Moy, and Robert McVay.
Killed by Code: Software Transparency in Implantable Medical Devices (Software Freedom Law Center, 21 July 2010), available at: https://www.softwarefreedom.org/resources/2010/transparent-medical-devices.pdf

Schulzrinne, H., et al., "Geolocation Policy: A Document Format for Expressing Privacy Preferences for Location Information", The Internet Engineering Task Force, Internet Draft, February 2009, available at: http://www.ietf.org/id/draft-ietf-geopriv-policy-21.txt

Welbourne, E., et al. *Challenges for Pervasive RFID-based Infrastructure*, PERTEC 2007, Workshop on Pervasive RFID/NFC Technology and Applications, 19 March 2007, available at: http://rfid.cs.washington.edu/images/welbourne-pertec-07.pdf

Williams, Lorraine C. *A Discussion of the Importance of Key Length in Symmetric and Asymmetric Cryptography*, SANS Institute, GIAC practical repository, 2002, available at: http://www.giac.org/certified_professionals/practicals/gsec/0848.php

Williams, Mary-Anne. *Privacy Management, The Law and Global Business Strategies: A Case for Privacy Driven Design*, Innovation and Enterprise Research Laboratory, University of Technology, Sydney, 2009.

REPORTS

Cave, J., C. van Oranje, R. Schindler, A. Ahehabi, PH-B. Brutscher, N. Robinson, *Trends in connectivity technologies and their socio-economic impacts, Final report of the study*: Policy Options for the Ubiquitous Internet Society, (RAND Europe, July 2009).

Crowd control technologies, An appraisal of technologies for political control, Final Report to the STOA (Omega Foundation, 2000), available at: http://www.europarl.europa.eu/stoa/publications/studies/19991401a_en.pdf

Wood, David Murakami (ed.). *A Report on the Surveillance Society* (2006).

PART 1: Identification Roadmap 2005 – 2020, Biometrics Technology Roadmap for Person Identification within the Police Service, Police IT Organization.

Martin Gill, Angela Spriggs et al., "The impact of CCTV: fourteen case studies", Home Office Online Report 15/05, available at: http://www.homeoffice.gov.uk/rds/pdfs05/rdsolr1505.pdf

FTC Final Report, "Protecting Consumer Privacy in an Era of Rapid Change", March 2012, available at: http://ftc.gov/os/2012/03/120326privacyreport.pdf

Privacy By Design Report, Information Commissioner's Office, 2008, available at: http://www.ico.gov.uk/upload/documents/pdb_report_html/privacy_by_design_report_v2.pdf

Canadian Privacy Commissioner's report on Genetic Testing and Privacy (1992).
Jay Hoofnagle, Chris. *Privacy Self Regulation: A Decade of Disappointment*, EPIC, 4 March 2005, available at: http://epic.org/reports/decadedisappoint.pdf

Digital Confidence – Searching the next wave of digital growth (Booz & Company, Liberty Global Policy Series, 2008.

The Use of RFID for Human Identification: A Draft Report from DHS Emerging Applications and Technology Subcommittee to the Full Data Privacy and Integrity Advisory Committee, Version 1.0, available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_rpt_rfid_draft.pdf

The Use of RFID for Human Identify Verification, Report No. 2006-02, Data Privacy & Integrity Advisory Committee, Adopted 6 December 2006, available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf

RFID: Radio Frequency IDentification: Applications and Implications for Consumers: A Workshop Report From the Staff of the Federal Trade Commission [hereinafter called "FTC staff report on RFID"], FTC, March 2005, available at: http://www.ftc.gov/os/2005/03/050308rfidrpt.pdf

DHS Privacy Office Annual Report to Congress, July 2007-July 2008.

Opinion of the European Group on Ethics in Science and New Technologies to the European Commission, Opinion No. 20, 16/03/2005.

Dilemmas of Privacy and Surveillance: Challenges of Technological Change (The Royal Academy of Engineering, London, 2007), available at: http://www.raeng.org.uk/policy/reports/pdf/dilemmas_of_privacy_and_surveillance_report.pdf

"A Holistic Privacy Framework for RFID Applications", Future of Identity in the Information Society (FIDIS), Simone Fischer-Hübner and Hans Hedbom (eds.), Deliverable D12.3.

Wilamovska, Anna-Marie. et al. *Study on the requirements and options for RFID application in healthcare*, RAND Europe (2008), Prepared for the Directorate General Information Society and Media of the European Commission.

American Medical Association, CEJA Report 5-A-07, available at: http://www.ama-assn.org/ama1/pub/upload/mm/467/ceja5a07.doc

Report of the Council on Ethical and Judicial Affairs, CEJA Report 5-A-07, available at: http://www.ama-assn.org/ama1/pub/upload/mm/467/ceja5a07.doc

Sedlak, Andrea J., et al. "National Estimates of Missing Children: An Overview" in *National Incidence Studies of Missing, Abducted, Runaway, and Thrownaway Children* (Office of Juvenile Justice and Delinquency Prevention, Office of Justice Programs, U.S. Department of Justice, October 2002), pp. 4-7, available at: http://www.ncjrs.gov/pdffiles1/ojjdp/196465.pdf

Report to Congress regarding the Terrorism Information Awareness Program, DARPA, 20 May 2003.

The Use of RFID for Human Identify Verification, Report No. 2006-02, Data Privacy & Integrity Advisory Committee, Adopted 6 December 2006, available at: http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_12-2006_rpt_RFID.pdf

van Kranenburg, Rob. *The Internet of Things: A critique of ambient technology and the all-seeing network of RFID*, Network Notebooks 02, Institute of Network Cultures (2008).

van Blarkom, G.W., J.J. Borking, J.G.E. Olk (eds.). *The Handbook of Privacy and Privacy-Enhancing Technologies: The Case of Intelligent Software Agents* (2003).

Digital Confidence – Searching the next wave of digital growth (Booz & Company, Liberty Global Policy Series, 2008).

Application of a methodology designed to assess the adequacy of the level of protection of individuals with regard to processing personal data: Test of the method on several categories of transfer, Final Report presented by the University of Edinburgh on behalf of: Charles D. Raab, Colin J. Bennett, Robert M. Gellman, and Nigel Waters, September 1998, European Commission Tender No. XV/97/18/D, available at: http://ec.europa.eu/justice/policies/privacy/docs/studies/adequat_en.pdf

Presidential Report on Radiation Protection Advice: Screening of Humans for Security Purposes Using Ionizing Radiation Scanning Systems (National Council on Radiation Protection and Measurements, 2003), available at: http://www.fda.gov/ohrms/dockets/ac/03/briefing/3987b1 pres-report.pdf

Friedewald, M., R. Lindner & D. Wright (eds.), "Policy Options to Counteract Threats and Vulnerabilities in Ambient Intelligence", SWAMI Deliverable D3: A report of the SWAMI consortium to the European Commission under contract 006507, June 2006, (Draft version), available at: http://www.isi.fhg.de/publ/downloads/isi06b24/SWAMI_D3_030706.pdf

Trust in the Information Society: Research and Innovation on Security, Privacy and Trustworthiness in the Information Society, A Report of the Advisory Board RISEPTIS, 2009.

Summary

With a focus on the growing development and deployment of the latest technologies that threaten privacy, the PhD dissertation argues that the US and UK legal frameworks, in their present form, are inadequate to defend privacy and other civil liberties against the intrusive capabilities of body scanners, CCTV microphones and loudspeakers, human-implantable microchips, and other privacy-intrusive technologies. While there are benefits derived from the use of these technologies in terms of public security, for instance, these benefits do not necessarily need to come at the expense of privacy and liberty overall. The interests of privacy, liberty and security can be balanced and safeguarded concurrently. In order to accomplish this worthy objective, new laws must further regulate directly and proactively the design and manufacture of these privacy-intrusive technologies in the first place, rather than only regulate their use or operation. Manufacturer-level rules/regulations should, therefore, require the incorporation of the fundamental privacy principles through what is known as "Privacy by Design".

Samenvatting

Privacy-Invading Technologies: Bescherming van de Privacy, Vrijheid en Veiligheid in de 21ste eeuw.

In het licht van de toenemende ontwikkeling en inzet van de nieuwste privacybedreigende technologieën, concludeert dit proefschrift dat de wettelijke kaders in zowel de Verenigde Staten als het Verenigd Koninkrijk in hun huidige vorm niet toereikend zijn om de privacy en andere burgerlijke vrijheden te beschermen/verdedigen. Het betreft technologieën die kunnen binnendringen in de persoonlijke levenssfeer zoals bodyscanners, CCTV microfoons en luidsprekers, in mensen implanteerbare microchips en andere technologieën die inbreuk maken op de privacy. Hoewel het gebruik van deze technologieën voordelen oplevert in bijvoorbeeld het belang van de openbare veiligheid, worden dergelijke voordelen niet vanzelfsprekend ook behaald op het vlak van de privacy en algemene vrijheden. De belangen van de privacy en vrijheden aan de ene kant en de openbare veiligheid aan de andere kant kunnen evenwel in evenwicht worden gebracht en tegelijkertijd worden gewaarborgd. Voor het kunnen behalen van de ambitie van zo een evenwicht is nieuwe wetgeving nodig: wetgeving die direct en proactief het ontwerp en de ontwikkeling van inbreukmakende technologieën reguleert in plaats van zich enkel te richten op het reguleren van de operationele werking en het gebruik ervan. Regulering op het niveau van de productie zal daarom ook eisen moeten stellen die fundamentele privacyprincipes beschermen door middel van wat bekend staat als “Privacy by Design”.

Curriculum Vitae

Demetrius Klitou (1981, U.S.A.) has a BA in international relations and a MA in diplomatic studies. He subsequently obtained a LL.M. in public international law from Leiden University. His academic background has significantly focused on human rights law/theory and policymaking. He is currently serving as a consultant, specialized in the non-technological aspects of technology policies and R&D, innovation activities, internationalization of research, policy development and project management. He previously worked at the European Commission (DG Information Society & Media), where he dealt with ICT and societal challenges and contributed to information society/digital agenda policies. Demetrius conducted his PhD research at Leiden University, Centre for Law in the Information Society (eLaw@Leiden). The research was entirely self-funded.